ESET NOD32 ANTIVIRUS 6

Guia do Usuário

(destinado ao produto versão 6.0 e posterior)

Microsoft® Windows® 8 / 7 / Vista / XP / Home Server

Clique aqui para fazer download da versão mais recente deste documento

ESET NOD32 ANTIVIRUS

Atendimento ao cliente mundial www.eset.com/support

REV. 12/3/2012

Índice

1. ESET NOD32 Antivirus 6

O ESET NOD32 Antivirus 6 representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ThreatSense® utiliza velocidade e precisão para manter a segurança do seu computador. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

O ESET NOD32 Antivirus 6 é uma solução de segurança completa que combina proteção máxima e impacto mínimo no sistema. Nossas tecnologias avançadas usam inteligência artificial para impedir infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outras ameaças sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

Recursos e benefícios

Antivírus e antispyware	Detecta e limpa proativamente mais vírus, worms, cavalos de troia e rootkits conhecidos e desconhecidos. A tecnologia de detecção heurística avançada sinalizada até mesmo malware nunca visto antes, protegendo você de ameaças desconhecidas e neutralizando-as antes que possam causar algum dano. A proteção de acesso à Web e a proteção antiphishing funcionam monitorando a comunicação entre os navegadores da Internet e servidores remotos (incluindo SSL). A Proteção do cliente de email fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP.
Atualizações regulares	Atualizar o banco de dados de assinatura de vírus e os módulos do programa periodicamente é o melhor método para se obter o nível máximo de segurança em seu computador.
ESET Live Grid (Reputação potencializada pela nuvem)	Você pode verificar a reputação dos arquivos e dos processos em execução diretamente do ESET NOD32 Antivirus.
Controle de mídia removível	Rastreia automaticamente todas as unidades flash USB, cartões de memória e CDs/DVDs. Bloqueia mídia removível com base no tipo de mídia, fabricante, tamanho e outros atributos.
Funcionalidade do HIPS	Você pode personalizar o comportamento do sistema em mais detalhes; especifique regras para o registro do sistema, processos e programas ativos e ajuste sua postura de segurança.
Modo de jogador	Adia todas as janelas pop-up, atualizações ou outras atividades que exijam muitos recursos do sistema, a fim de conservar recursos do sistema para jogos ou outras atividades de tela inteira.

Uma licença precisa estar ativa para que os recursos do ESET NOD32 Antivirus estejam operacionais. Recomenda-se que você renove sua licença várias semanas antes de a licença do ESET NOD32 Antivirus expirar.

1.1 O que há de novo

Reversão para banco de dados de assinatura de vírus anterior

Caso suspeite que uma nova atualização do banco de dados de vírus ou módulo do produto esteja instável ou corrompida, será possível reverter para uma versão anterior e desativar quaisquer atualizações por um período de tempo definido.

Proteção antiphishing aprimorada

O ESET NOD32 Antivirus exibirá uma notificação de aviso com várias opções quando um navegador da web tentar acessar sites ou domínios catalogados no banco de dados de malware da ESET.

Rastreamento completo regular

Para maior segurança, a versão 6 do ESET NOD32 Antivirus pode realizar regularmente um rastreamento completo do computador durante seu período ocioso. O rastreamento é otimizado para não ser executado quando o computador estiver fazendo uso de bateria.

O rastreamento completo regular ajuda a detectar ameaças inativas no computador e melhora as informações de nuvem da ESET sobre arquivos ou ameaças conhecidas ou desconhecidas.

Melhorias no rastreamento de arquivos baixados

Em versões anteriores, os arquivos baixados da Internet eram rastreados pela ESET somente depois que o download era concluído. A versão 6 do ESET NOD32 Antivirus rastreia tipos de arquivos específicos (p. ex., arquivos compactados) durante o processo de download, a fim de que o usuário não precise aguardar o processo de download ser concluído para que os arquivos sejam rastreados.

Notificações de aplicativos unificadas

O design e o layout de todas as janelas de notificação foram unificados na versão 6.

1.2 Requisitos do sistema

Para uma operação sem interrupções do ESET NOD32 Antivirus, o sistema deve atender aos seguintes requisitos de hardware e de software:

Microsoft® Windows® XP

400 MHz 32 bits (x86)/64 bits (x64)
128 MB de memória RAM do sistema
320 MB de espaço disponível
Super VGA (800 x 600)

Microsoft® Windows® 7, 8, Vista, Home Server

1 GHz 32 bits (x86)/64 bits (x64)
512 MB de memória RAM do sistema
320 MB de espaço disponível
Super VGA (800 x 600)

1.3 Prevenção

Quando você trabalhar com o computador, e especialmente quando navegar na Internet, tenha sempre em mente que nenhum sistema antivírus do mundo pode eliminar completamente o risco de ameaças e ataques. Para fornecer proteção e conveniência máximas, é essencial usar a solução antivírus corretamente e aderir a diversas regras úteis:

Atualização regular

De acordo com as estatísticas do ESET Live Grid, milhares de novas ameaças únicas são criadas todos os dias a fim de contornar as medidas de segurança existentes e gerar lucro para os seus autores - todas às custas dos demais usuários. Os especialistas no Laboratório de vírus da ESET analisam essas ameaças diariamente, preparam e publicam atualizações a fim de melhorar continuamente o nível de proteção de nossos usuários. Para garantir a máxima eficácia dessas atualizações, é importante que elas sejam configuradas devidamente em seu sistema. Para obter mais informações sobre como configurar as atualizações, consulte o capítulo Configuração da atualização.

Download dos patches de segurança

Os autores dos softwares maliciosos frequentemente exploram as diversas vulnerabilidades do sistema a fim de aumentar a eficiência da disseminação do código malicioso. Considerado isso, as empresas de software vigiam de perto quaisquer vulnerabilidades em seus aplicativos para elaborar e publicar atualizações de segurança, eliminando as ameaças em potencial regularmente. É importante fazer o download dessas atualizações de segurança à medida que são publicadas. Microsoft Windows e navegadores da web, como o Internet Explorer, são dois exemplos de programas para os quais atualizações de segurança são lançadas regularmente.

Backup de dados importantes

Os escritores dos softwares maliciosos não se importam com as necessidades dos usuários, e a atividade dos programas maliciosos frequentemente leva ao mau funcionamento de um sistema operacional e a ´perda de dados importantes. É importante fazer o backup regular dos seus dados importantes e sensíveis para uma fonte externa como um DVD ou disco rígido externo. Isso torna mais fácil e rápido recuperar os seus dados no caso de falha do sistema.

Rastreie regularmente o seu computador em busca de vírus

A detecção de mais vírus, cavalos de troia e rootkits conhecidos e desconhecidos é realizada pelo módulo Proteção em tempo real do sistema de arquivos. Isso significa que sempre que você acessar ou abrir um arquivo, ele será rastreado

quanto à atividade de malware. No entanto, recomendamos que você execute um rastreamento no computador inteiro pelo menos uma vez por mês, pois o malware varia, assim como as atualizações do banco de dados de assinatura de vírus são atualizadas diariamente.

Siga as regras básicas de segurança

Essa é a regra mais útil e eficiente de todas - seja sempre cauteloso. Hoje, muitas ameaças exigem a interação do usuário para serem executadas e distribuídas. Se você for cauteloso ao abrir novos arquivos, economizará tempo e esforço consideráveis que, de outra forma, seriam gastos limpando as ameaças do seu computador. Aqui estão algumas diretrizes úteis:

- Não visite sites suspeitos com inúmeras pop-ups e anúncios piscando.
- Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Use somente programas seguros e somente visite sites da Internet seguros.
- Seja cauteloso ao abrir anexos de e-mail, especialmente aqueles de mensagens spam e mensagens de remetentes desconhecidos.
- Não use a conta do Administrador para o trabalho diário em seu computador.

2. Instalação

Há vários métodos para a instalação do ESET NOD32 Antivirus em seu computador. Os métodos de instalação podem variar dependendo do país e meio de distribuição:

- O instalador Live pode ser obtido por download do site da ESET. O pacote de instalação é universal para todos os idiomas (escolha um idioma desejado). O próprio instalador Live é um arquivo pequeno; arquivos adicionais necessários para instalar o ESET NOD32 Antivirus serão baixados automaticamente.
- Instalação off-line - Este tipo de instalação é uasdo ao instalar de um CD/DVD do produto. Ele usa um arquivo *.msi*, que é maior do que o arquivo do instalador Live e não exige uma conexão com a Internet ou arquivos adicionais para a conclusão da instalação.

Importante: Verifique se não há algum outro programa antivírus instalado no computador antes de instalar o ESET NOD32 Antivirus . Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso artigo da base de conhecimento da ESET para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).

2.1 Instalador Live

Assim que você tiver feito download do pacote de instalação do *Instalador Live*, dê um duplo clique no arquivo de instalação e siga as instruções passo a passo na janela do instalador.

Importante: Para esse tipo de instalação, você deverá estar conectado à Internet.

Selecione seu idioma desejado no menu suspenso **Selecione o idioma do produto** e clique em **Instalar**. Aguarde alguns momentos para o download dos arquivos de instalação.

Depois de aceitar o **Contrato de licença para o usuário final**, será solicitado que você configure o **ESET Live Grid**. O ESET Live Grid ajuda a assegurar que a ESET seja informada continua e imediatamente sobre novas infiltrações para proteger seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de vírus da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus.

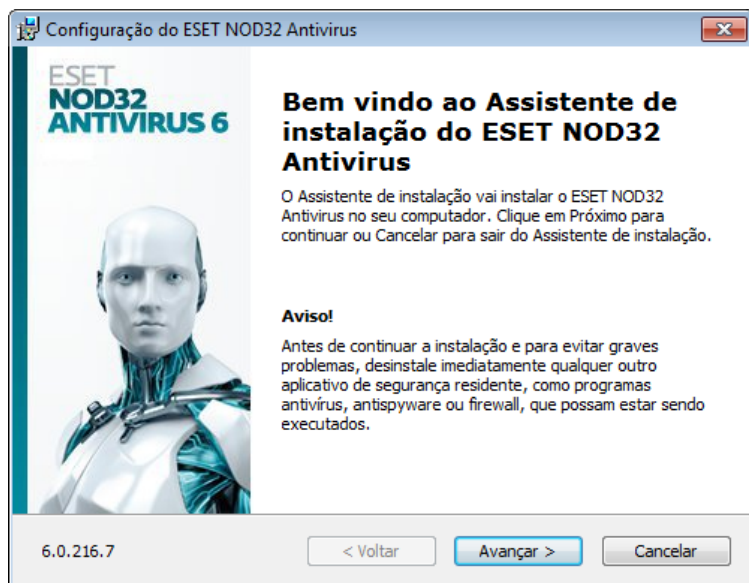
Por padrão, a opção **Sim, desejo participar** está selecionada, o que ativará esse recurso.

Por padrão, o ESET NOD32 Antivirus é instalado na pasta mostrada ao lado de **Pasta de destino**. Para especificar o local no qual o ESET NOD32 Antivirus será instalado, clique em **Alterar...**.

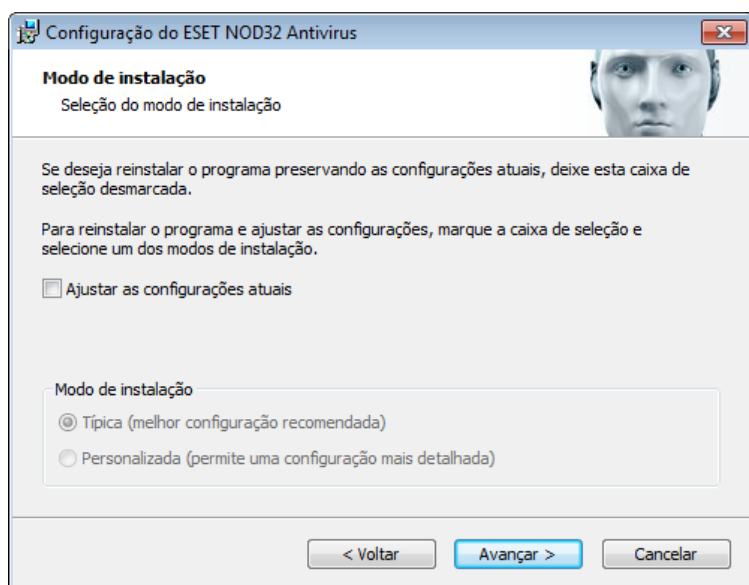
A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Consulte o capítulo Aplicativos potencialmente indesejados para obter mais detalhes.

Clique em **Avançar** para iniciar o processo de instalação.

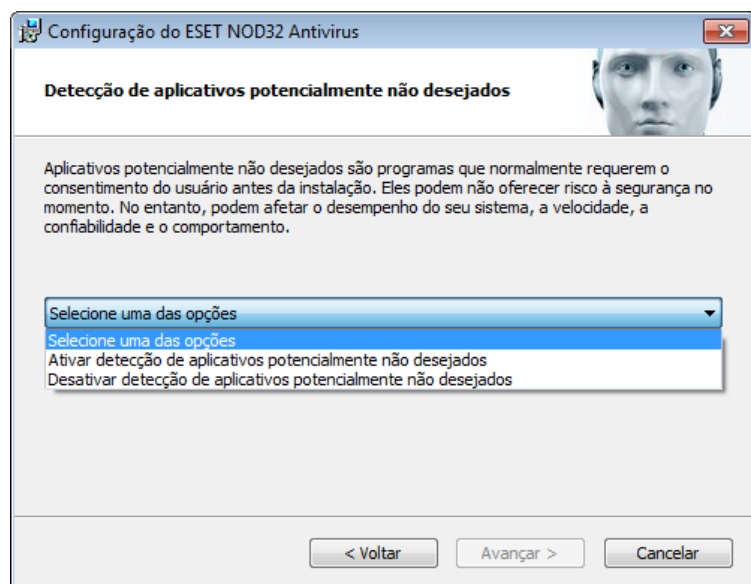
2.2 Instalação off-line

Assim que você iniciar o pacote de instalação off-line (.msi), o assistente de instalação o guiará pelo processo de configuração.

Primeiro, o programa verifica para ver há uma versão mais nova do ESET NOD32 Antivirus disponível. Se uma versão mais recente for encontrada, você será notificado na primeira etapa do processo de instalação. Se selecionar a opção **Fazer download e instalar nova versão**, a nova versão será obtida por download e a instalação continuará. Em seguida, o Contrato de licença de usuário final será exibido. Leia-o e clique em **Aceitar** para confirmar a sua aceitação do Contrato de licença de usuário final. Depois que você aceitar, a instalação continuará em uma das seguintes formas:

1. Se você estiver instalando o ESET NOD32 Antivirus em um computador pela primeira vez, verá a janela a seguir. Aqui, você pode escolher entre uma Instalação típica e uma Instalação personalizada e continuar.

2. Se você estiver instalando o ESET NOD32 Antivirus em uma versão anterior, poderá optar por usar as configurações do seu programa atual para sua nova instalação; ou você poderá marcar a caixa de seleção **Ajustar as configurações atuais** e escolher entre os dois modos de instalação mencionados anteriormente (personalizada ou típica).

2.2.1 Instalação típica

O modo de instalação Típica inclui as opções de configuração apropriadas para a maioria dos usuários. Essas configurações proporcionam excelente segurança, configuração fácil e alto desempenho do sistema. O modo de instalação típica é a opção padrão e é recomendada para usuários que não têm exigem configurações específicas.

Para obter mais instruções sobre etapas de instalação, o **ESET Live Grid** e a opção **Detecção de aplicativos potencialmente não desejados**, siga as instruções na seção mencionada anteriormente (consulte "Instalador Live").

Clique em **Instalar** para confirmar a instalação depois de ter concluído.

2.2.2 Instalação personalizada

O modo de instalação personalizada é destinado a usuários experientes e que desejam modificar configurações avançadas durante a instalação.

Após selecionar este modo de instalação e clicar em **Avançar**, será preciso definir um local de destino para a instalação. Por padrão, o programa é instalado no seguinte diretório:

C:\Program Files\ESET\ESET NOD32 Antivirus

Clique em **Procurar...** para alterar o local (não recomendado).

Clique em **Avançar** e continue para configurar a conexão com a Internet. Se você usa um servidor proxy, ele deve ser configurado corretamente para que as atualizações das assinaturas de vírus funcionem. Se você não tiver certeza se deve usar um servidor proxy para se conectar à Internet, selecione **Utilizar as mesmas configurações que o Internet Explorer (Recomendado)** e clique em **Avançar**. Se você não utilizar um servidor proxy, selecione a opção **Eu não utilizo um servidor proxy**.

Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **usuário** e uma **senha** válidos a fim de obter acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Para fazer isso, clique em **Aplicar** e confirme a seleção.

Essa etapa de instalação permite designar como as atualizações automáticas do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes de programa**. Selecione a opção **Perguntar antes de fazer download dos componentes de programa** para exibir uma janela de confirmação sempre que o sistema tentar fazer download dos componentes de programa. Para fazer download automaticamente de atualizações dos componentes do programa, selecione a opção **Sempre atualizar componentes do programa**.

OBSERVAÇÃO: Após a atualização dos componentes do programa, geralmente é necessária a reinicialização do sistema. Recomendamos selecionar a opção **Se necessário, reiniciar o computador sem notificar**.

A próxima janela da instalação oferecerá a opção de definir uma senha para proteger as configurações do programa. Selecione a opção **Proteger as configurações por senha** e digite a sua senha nos campos **Nova senha** e **Confirmar nova senha**. Esta senha será solicitada em todas modificações ou acessos futuros no ESET NOD32 Antivirus. Quando ambos os campos de senha coincidirem, clique em **Avançar** para continuar.

Para concluir as próximas etapas de instalação, **ESET Live Grid** e **Detecção de aplicativos potencialmente não desejados**, siga as instruções na seção Instalador Live (consulte "Instalador Live").

Clique em **Instalar** na janela **Pronto para instalar** para concluir a instalação.

2.3 Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país, assim como os meios de distribuição (CD/DVD, página da web da ESET etc.).

Se você adquiriu uma versão do produto em um caixa no varejo, selecione a opção **Ativar usando uma Chave de ativação**. A Chave de Ativação está normalmente localizada no interior ou na parte posterior do pacote do produto. Para uma ativação bem-sucedida, a Chave de Ativação deve ser digitada conforme fornecida.

Se você recebeu um nome de usuário e uma senha, selecione a opção **Ativar utilizando um Usuário e Senha** e insira suas credenciais nos campos apropriados.

Se desejar avaliar o ESET NOD32 Antivirus antes de fazer uma aquisição, selecione a opção **Ativar licença de avaliação**. Insira seu nome e endereço de email para ativar o ESET NOD32 Antivirus por um período limitado. A licença de teste será enviada para seu email. As licenças de avaliação podem ser ativadas apenas uma vez por cliente.

Se você não tem uma licença e deseja adquirir uma, clique na opção **Comprar licença**. Isso o redirecionará para o site do seu distribuidor local da ESET.

Selecione a opção **Cancelar** se pretender avaliar rapidamente o nosso produto e não desejar ativá-lo imediatamente, ou se desejar ativar o produto depois.

Você pode ativar sua cópia do ESET NOD32 Antivirus diretamente a partir do programa. Clique no ícone Menu do programa no canto superior direito ou clique com o botão direito do mouse no ícone do ESET NOD32 Antivirus na bandeja do sistema e selecione **Ativação do produto...** no menu.

2.4 Inserção do usuário e da senha

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Isso somente será possível se o nome de usuário e a senha corretos forem digitados na **Configuração de atualização**.

Se você não inseriu o seu nome de usuário e senha durante a instalação, poderá inseri-los agora. Na janela principal do programa, clique em **Atualizar**, depois em **Ativação do produto...** e insira os dados da licença recebidos com o produto de segurança ESET na janela Ativação do produto.

Ao inserir seu **Nome de usuário** e **Senha**, é importante digitá-los exatamente como foram gravados:

- O nome de usuário e a senha fazem diferenciação de maiúsculas, minúsculas e hífens, se necessário.
- A senha tem dez caracteres e todos minúsculos.
- Não usamos a letra L em senhas (use o número um (1) no lugar da letra).
- Um 'O' mais alto é o número zero (0), um 'o' mais baixo é a letra 'o' minúscula.

Recomendamos que você copie e cole os dados do email de registro para garantir a precisão.

2.5 Atualização para uma versão mais recente

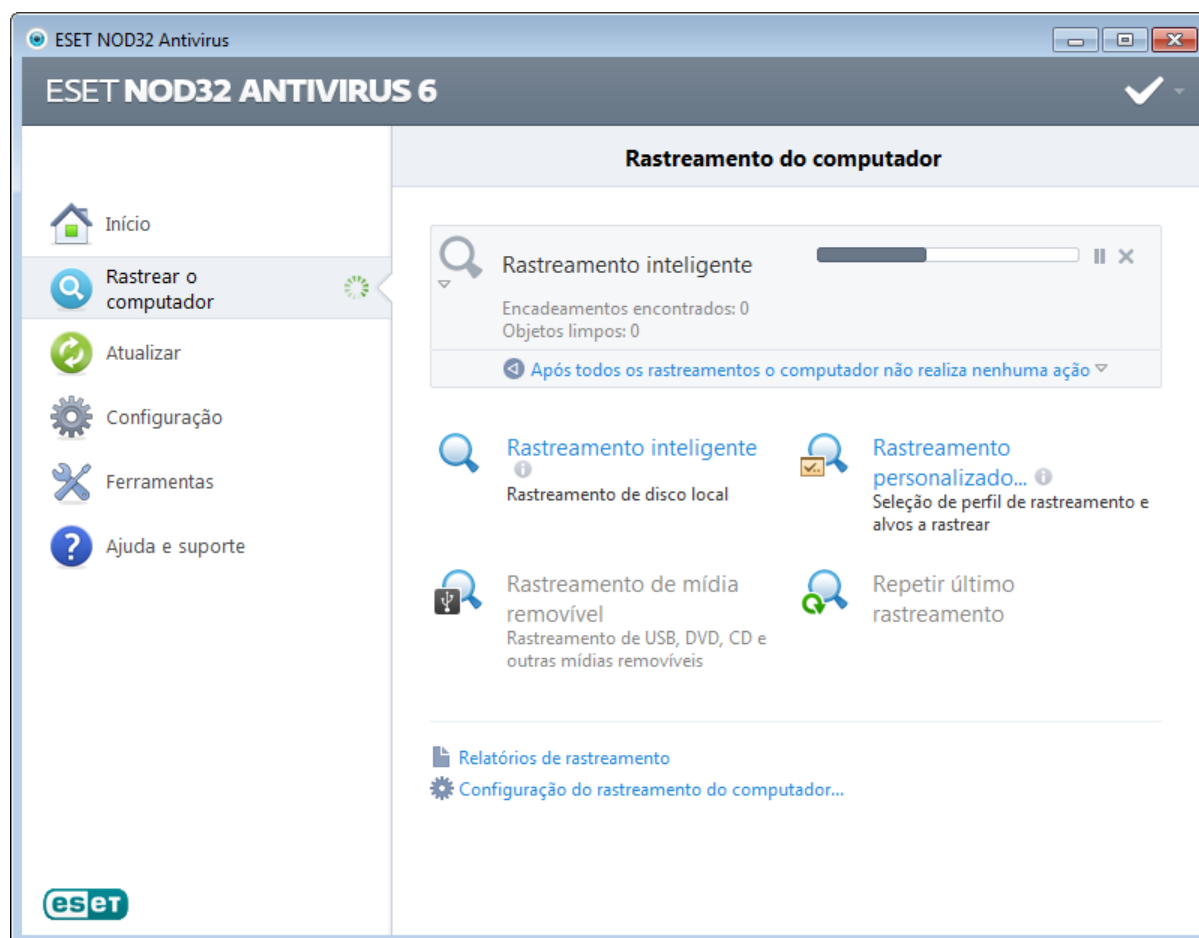
Versões mais recentes do ESET NOD32 Antivirus são lançadas para trazer aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos do programa. A atualização para uma versão mais recente pode ser feita de várias formas:

1. Automaticamente, por meio de uma atualização do programa
   Como a atualização do programa é distribuída para todos os usuários e pode ter impacto em determinadas configurações do sistema, ela é lançada depois de um longo período de testes para funcionar com todas as configurações de sistema possíveis. Se você precisar atualizar para uma versão mais recente imediatamente após ela ter sido lançada, use um dos métodos a seguir.

2. Manualmente, na janela do programa principal, clicando em **Instalar/Verificar se há atualizações** na seção **Atualizar**.

3. Manualmente, por meio de download e instalação de uma versão mais recente sobre a instalação anterior.
   No início da instalação, é possível optar por modificar as configurações atuais do programa marcando a caixa de seleção **Ajustar configurações atuais**.

2.6 Rastrear o computador

Após instalar o ESET NOD32 Antivirus, você deve executar um rastrear o computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, clique em **Rastreamento inteligente**. Para obter mais informações sobre rastreamentos do computador, consulte a seção Rastrear o computador.

3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET NOD32 Antivirus e de suas configurações básicas.

3.1 Introdução ao design da interface do usuário

A janela principal do ESET NOD32 Antivirus é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

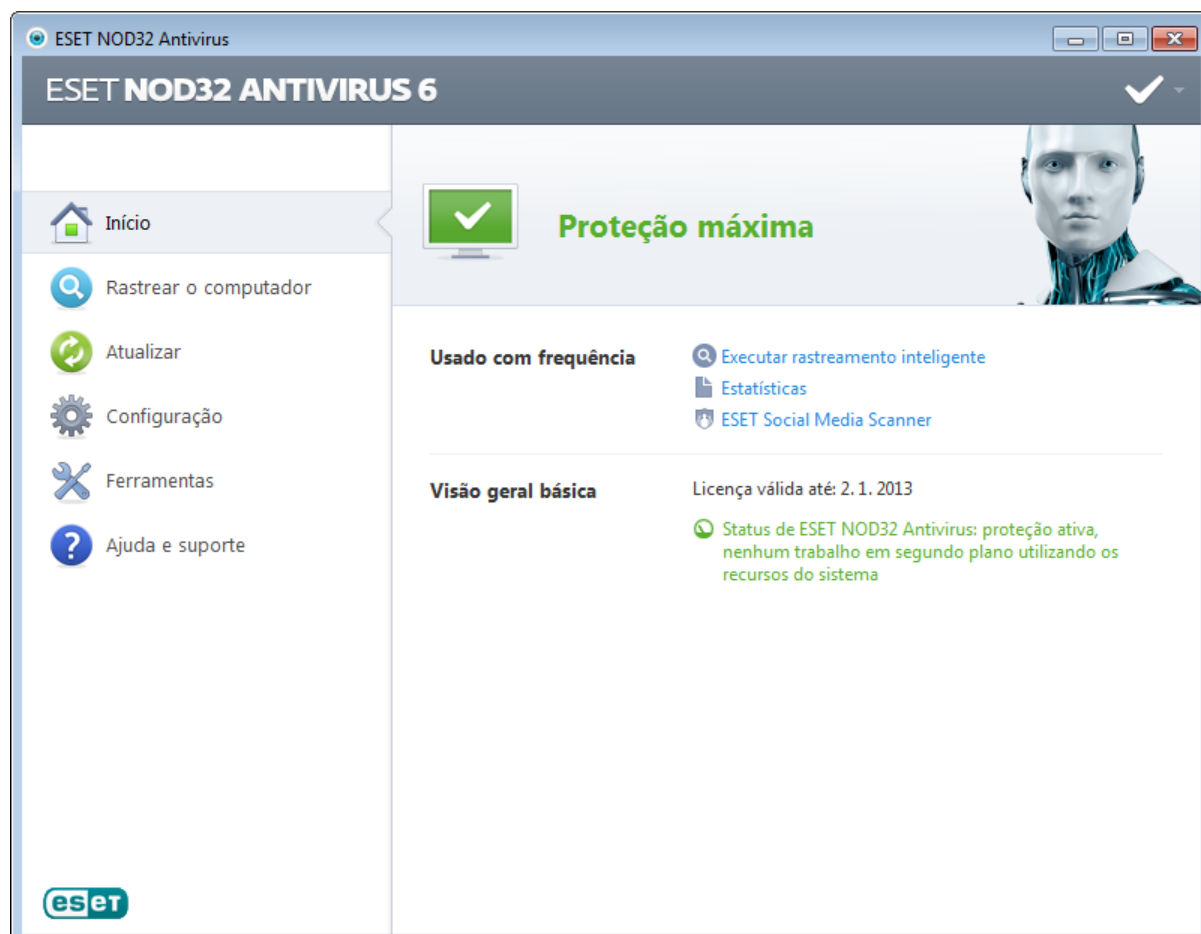
Início - Fornece informações sobre o status da proteção do ESET NOD32 Antivirus.

Rastrear o computador – Essa opção permite que você configure e inicie o Rastreamento inteligente ou o Rastreamento personalizado.

Atualizar - Exibe informações sobre as atualizações do banco de dados de assinatura de vírus.

Configuração - Selecione essa opção para ajustar o nível de segurança do computador, da Web e do email.

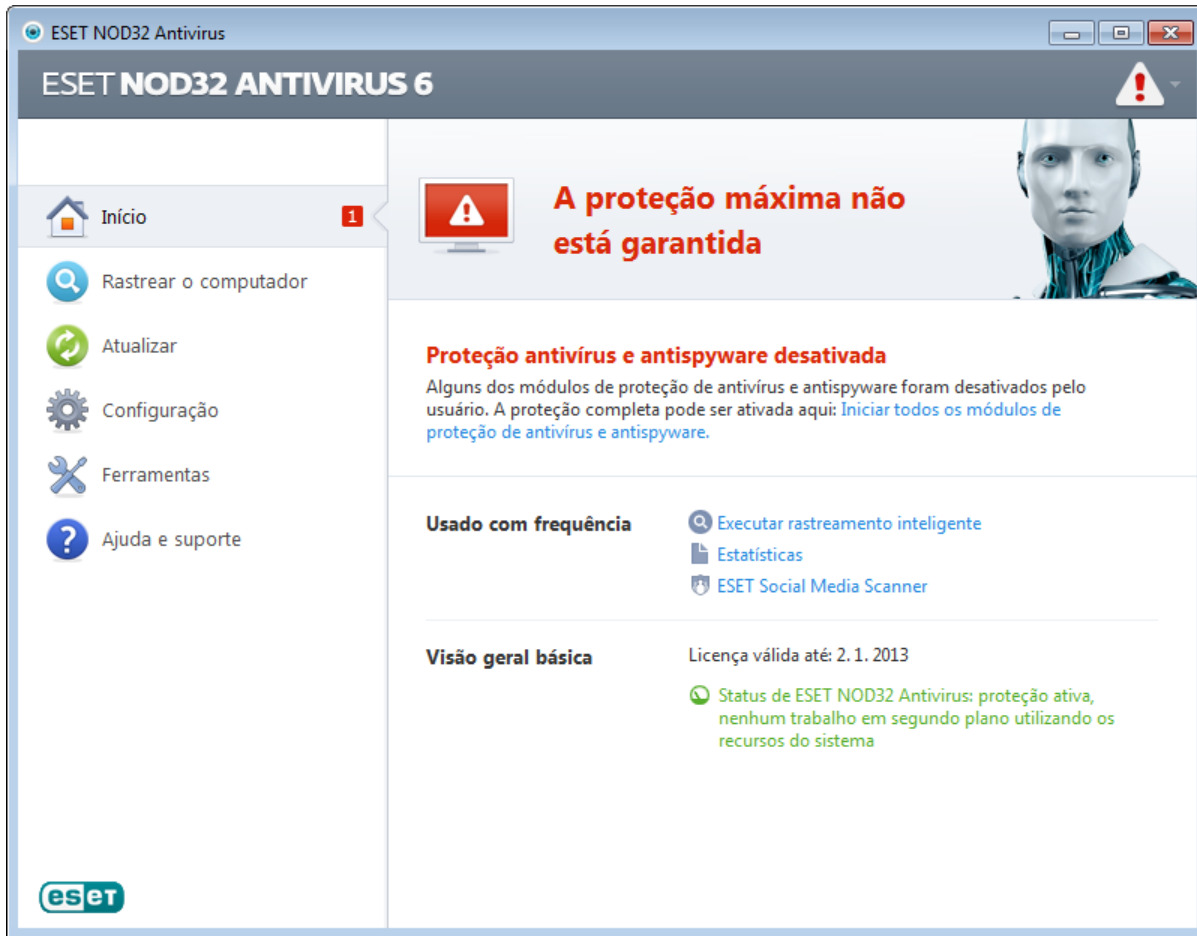
Ferramentas - Fornece acesso a arquivos de log, estatísticas de proteção, monitoramento de atividade, processos em execução, Agenda, quarentena, ESET SysInspector e ESET SysRescue.

Ajuda e suporte – Fornece acesso às páginas da ajuda, à Base de conhecimento da ESET e ao site e links da ESET para abrir uma solicitação de suporte ao Atendimento ao cliente.

A tela **Início** informa sobre a segurança e o nível de proteção atual do seu computador. O ícone verde de status de **Proteção máxima** indica que a proteção máxima está garantida.

A janela de status também exibe os recursos mais usados do ESET NOD32 Antivirus. As informações sobre a data de expiração do programa também podem ser encontradas aqui.

O que fazer se o programa não funcionar adequadamente?

Se os módulos ativados estiverem funcionando corretamente, o ícone do status de proteção estará verde. Um ponto de exclamação vermelho ou um ícone de notificação laranja indica que a máxima proteção não está garantida. Serão

exibidas informações adicionais sobre o status de proteção de cada módulo, bem como soluções sugeridas para a restauração da proteção total. Para alterar o status de módulos individuais, clique em **Configuração** e selecione o módulo desejado.

O ícone vermelho assinala problemas críticos - a proteção máxima do seu computador não está garantida. As possíveis razões são:

- Proteção em tempo real do sistema de arquivos desativada
- Banco de dados de assinatura de vírus desatualizado
- Produto não ativado
- A licença do produto expirou

O ícone laranja indica que a Proteção do cliente de email ou de acesso à web está desativada, que há um problema com a atualização do programa (banco de dados de assinatura de vírus desatualizado, impossível atualizar) ou que a data de expiração da licença está se aproximando.

Produto não ativado - Esse problema é assinalado por um ícone vermelho e uma notificação de segurança próxima ao item **Computador** (veja a captura de tela anterior). Você pode ativar o ESET NOD32 Antivirus no menu do programa clicando na opção **Ativação do produto...**. O menu do programa está localizado no canto superior direito da janela principal do programa.

Proteção antivírus e antispyware desativada - Esse problema é assinalado por um ícone vermelho e uma notificação de segurança próxima ao item **Computador** (veja a captura de tela anterior). Você pode reativar a proteção antivírus e antispyware clicando em **Iniciar todos os módulos de proteção antivírus e antispyware**.

Proteção do acesso à web desativada - Esse problema é assinalado por um ícone amarelo com um "i" e o status **Notificação de segurança**. Você pode reativar a proteção do acesso à web clicando na notificação de segurança e selecionando **Ativar proteção do acesso à web**.

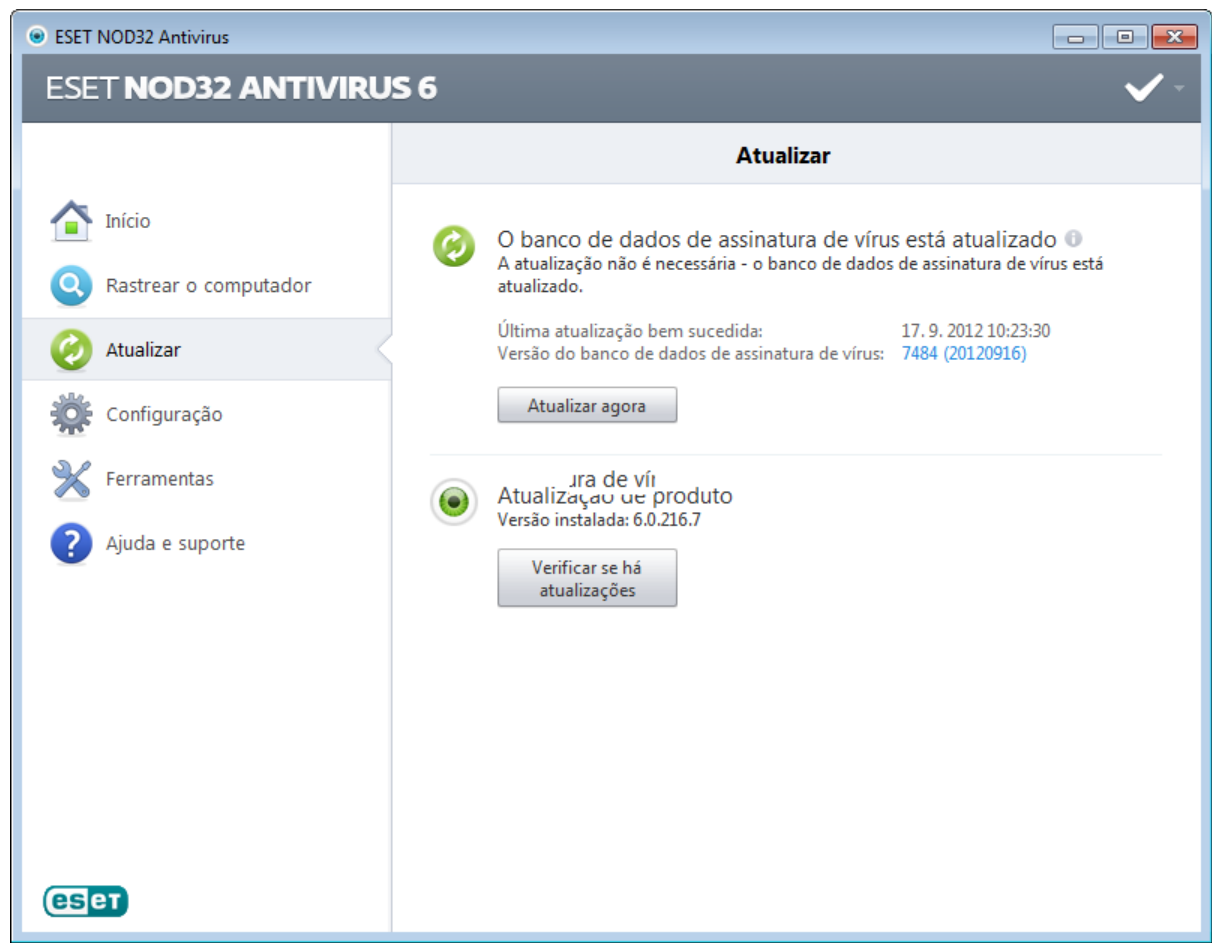
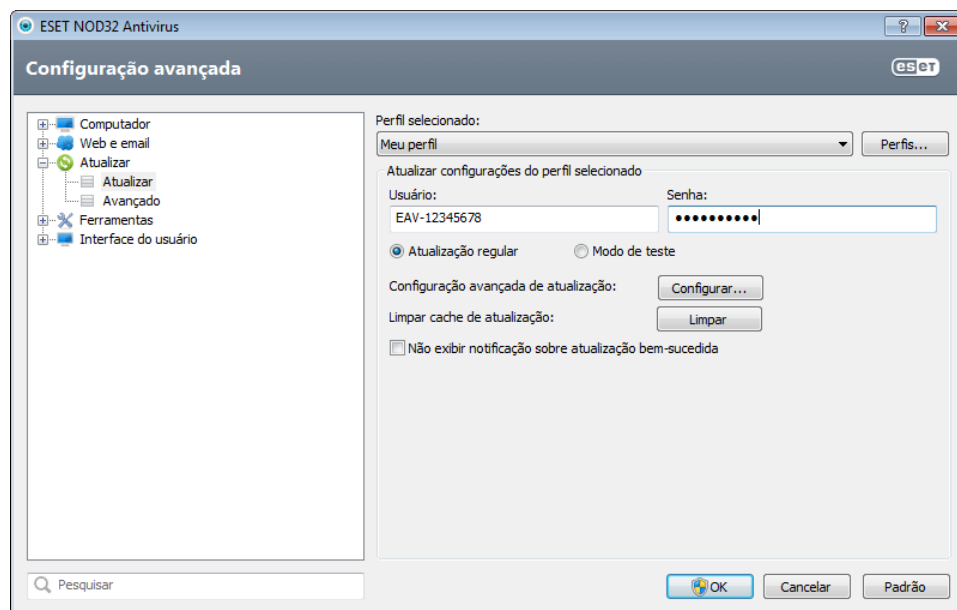
Sua licença expirará em breve - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação ao lado do relógio do sistema. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção ficará vermelho.

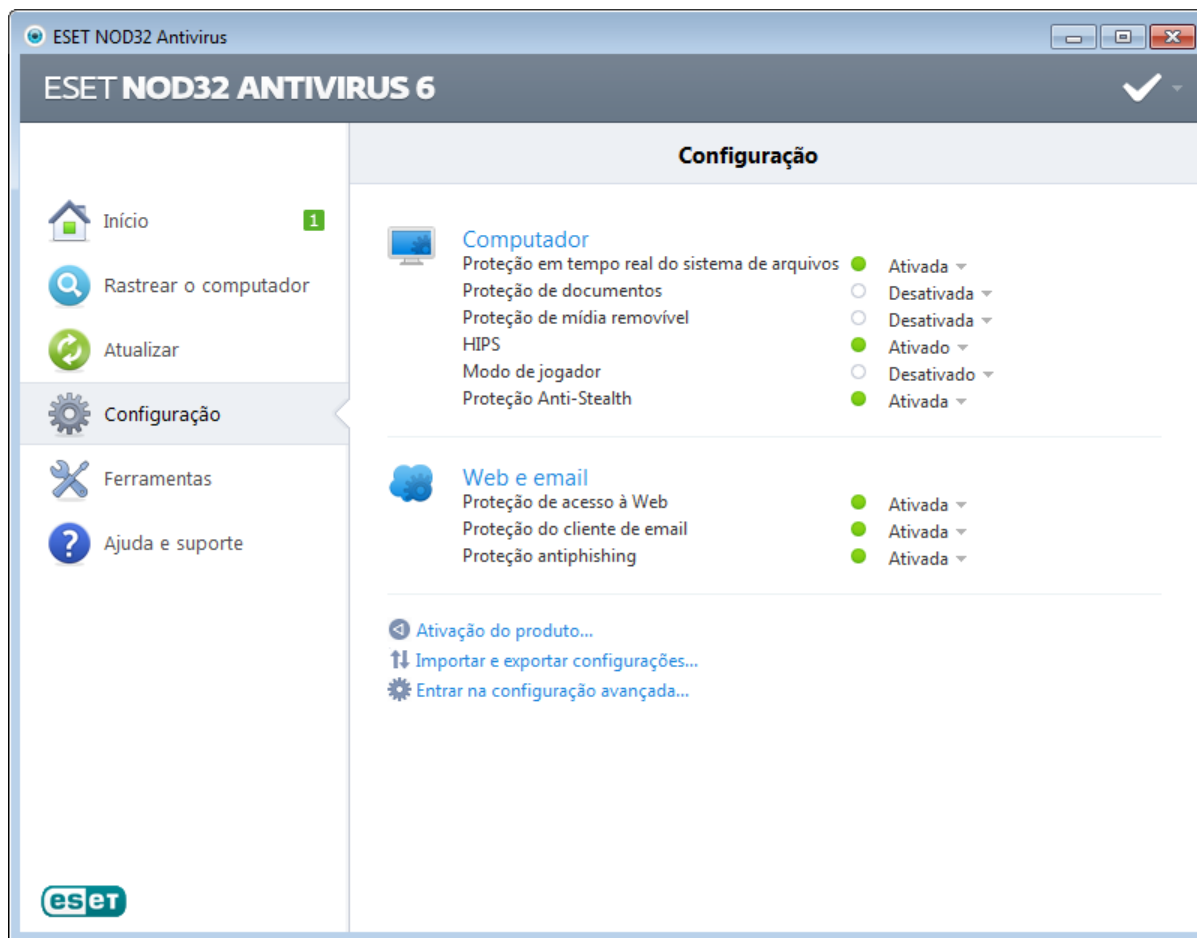
Licença expirada – Isso é indicado pelo ícone do status de proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Recomendamos que você siga as instruções da janela de alerta para renovar sua licença.

Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na Base de conhecimento da ESET. Se precisar de assistência, entre em contato com o Atendimento ao Cliente da ESET. O Atendimento ao Cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a encontrar uma solução.

3.2 Atualizações

A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes na proteção completa do seu sistema contra códigos maliciosos. Dê atenção especial à sua configuração e operação. No menu principal, clique em **Atualizar** e em **Atualizar banco de dados de assinatura de vírus** para verificar se há uma atualização do banco de dados de assinatura de vírus.

Se o nome de usuário e a senha não foram fornecidos durante a ativação do ESET NOD32 Antivirus, o sistema solicitará esses dados agora.

A janela Configuração avançada (no menu principal, clique em **Configuração** e escolha a opção **Entrar na configuração avançada...**, ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Atualizar** na árvore Configuração avançada à esquerda. O menu suspenso **Atualizar servidor** estará esmaecido e configurado como **Escolher automaticamente**. Para configurar as opções avançadas de atualização, como o modo de atualização, o acesso ao servidor proxy e as conexões de rede, clique em **Configuração...**. .

4. Trabalhar com o ESET NOD32 Antivirus

As opções de configuração do ESET NOD32 Antivirus permitem ajustar os níveis de proteção do computador.

O menu **Configuração** contém as seguintes opções:

- **Computador**
- **Web e email**

Clique em qualquer componente para ajustar as configurações avançadas do módulo de proteção correspondente.

A configuração da proteção do **Computador** permite ativar ou desativar os seguintes componentes:

- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **Proteção de documentos** - O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, como, por exemplo, elementos do Microsoft ActiveX.
- **Proteção da mídia removível** - Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e seleciona como o usuário pode acessar e trabalhar com um determinado dispositivo (CD/DVD/USB...).
- **HIPS** - O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo de jogos** – Ativa ou desativa o Modo de jogos. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela principal será exibida em laranja após a ativação do Modo de jogos.
- **Proteção Anti-Stealth** - detecta programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional e técnicas comuns de testes.

A configuração da proteção **Web e email** permite ativar ou desativar os seguintes componentes:

- **Proteção do acesso à web** - Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção do cliente de email** - Monitora a comunicação recebida através dos protocolos POP3 e IMAP.
- **Proteção antiphishing** - Filtra sites suspeitos de distribuir conteúdo com objetivo de manipular usuários para que enviem informações confidenciais.

OBSERVAÇÃO: a proteção de documentos também estará no estado **Ativado** depois de ativar a opção (**Entrar na configuração avançada...** (F5) > **Computador** > **Antivírus e antispyware** > **Proteção de documentos** > **Integrar ao sistema**).

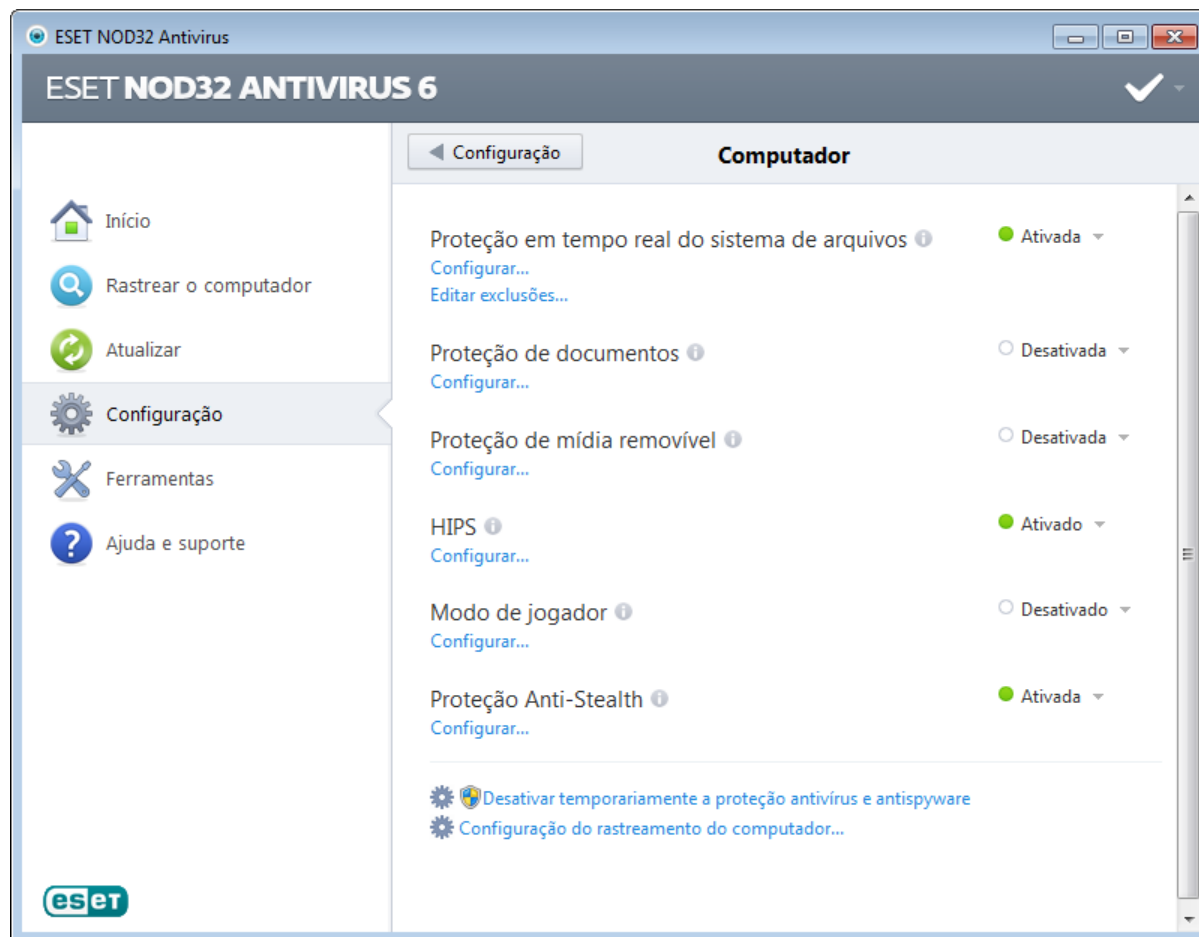
Para reativar a proteção do componente de segurança desativado, clique em **Desativado** e então em **Ativar**.

OBSERVAÇÃO: Ao desabilitar a proteção usando este método, todas as partes com deficiência de proteção serão ativadas após a reinicialização do computador.

Existem opções adicionais na parte inferior da janela de configuração. Use o link **Ativação do produto...** para abrir o formulário de registro que ativará o seu produto de segurança da ESET e enviará a você um email com seus dados de autenticação (nome de usuário e senha). Para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações...**.

4.1 Computador

O módulo **Computador** pode ser encontrado no painel **Configuração** depois de clicar em **Computador**. Essa janela mostra uma visão geral de todos os módulos de proteção. Para desativar os módulos individuais temporariamente, clique em **Ativado** > **Desativar para...** ao lado do módulo desejado. Observe que essa ação pode diminuir a proteção do seu computador. Para acessar as configurações detalhadas para cada módulo, clique em **Configurar...**.

Clique em **Editar exclusões...** para abrir a janela de configuração Exclusão, que permite a exclusão de arquivos e pastas do rastreamento.

Desativar temporariamente a proteção antivírus e antispyware - Desativa todos os módulos de proteção antivírus e antispyware. Quando você desativar a proteção, a janela **Desativar a proteção temporariamente** será aberta, permitindo que você determine por quanto tempo a proteção será desativada selecionando um valor no menu suspenso **Intervalo de tempo**. Clique em **OK** para confirmar.

Configuração do rastreamento do computador... - Clique para ajustar os parâmetros do Scanner sob demanda (rastreamento executado manualmente).

4.1.1 Antivírus e antispyware

A proteção de antivírus e antispyware protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la, primeiro bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

As opções do scanner para todos os módulos de proteção (p. ex., Proteção em tempo real do sistema de arquivos, Proteção do acesso à web, ...) permitem que você ative ou desative a detecção do seguinte:

- Os **Aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo.
  Leia mais sobre esses tipos de aplicativos no glossário.
- **Aplicativos potencialmente inseguros** refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos. Exemplos de aplicativos potencialmente inseguros incluem ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.
  Leia mais sobre esses tipos de aplicativos no glossário.
- **Aplicativos potencialmente suspeitos** incluem programas compactados com empacotadores ou protetores. Esses tipos de programas são frequentemente explorados por autores de malware para impedir a detecção.

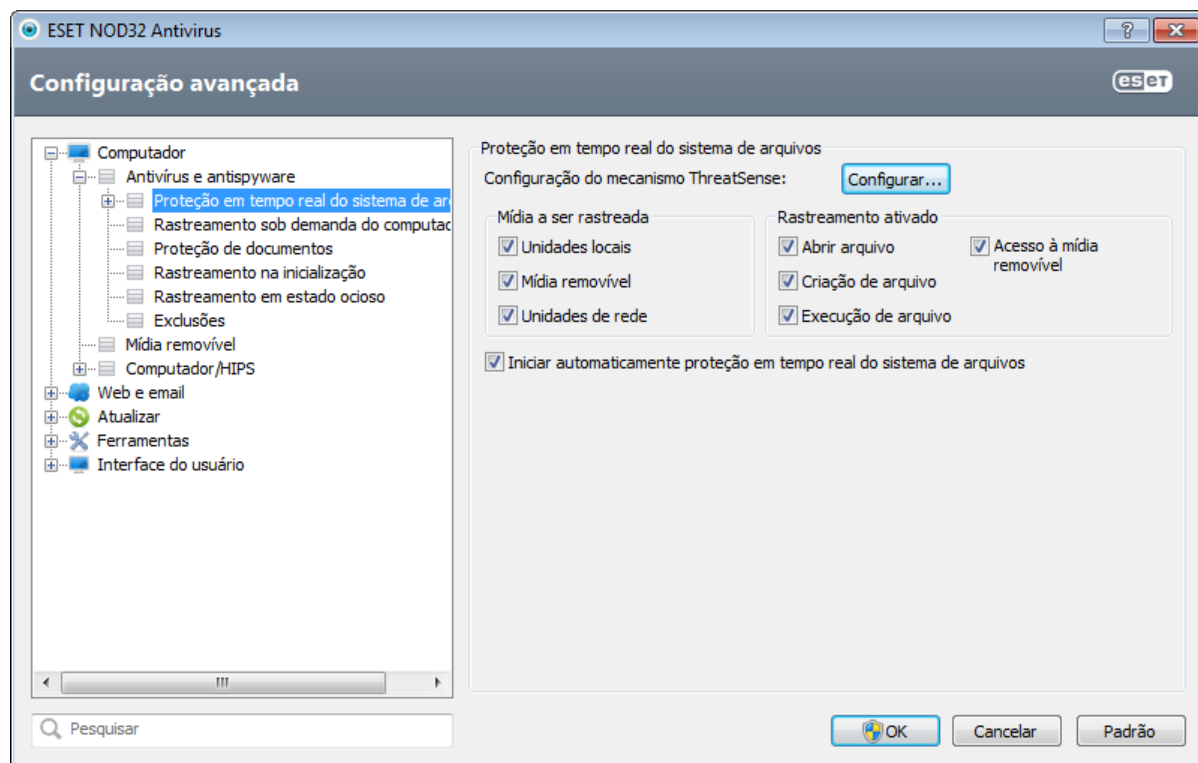
A tecnologia Anti-Stealth é um sistema sofisticado que fornece a detecção de programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

4.1.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense), a proteção em tempo real do sistema de arquivos pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Para garantir o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é configurado usando a **Otimização inteligente**. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Depois, clique no botão **Configuração...** ao lado de **Configuração de parâmetros do mecanismo ThreatSense**, clique em **Outros** e marque ou desmarque a opção **Ativar otimização inteligente**.

Por padrão, a proteção em tempo real do sistema de arquivos é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outra proteção em tempo real), a proteção em tempo real pode ser encerrada desmarcando a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**.

Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças:

Unidades locais - Controla todas as unidades de disco rígido do sistema.
Mídia removível - Disquetes, CD/DVDs, dispositivos de armazenamento USB, etc.
Unidades de rede - Rastreia todas as unidades mapeadas.

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador:

- **Abertura de arquivo** - Ativa ou desativa o rastreamento de arquivos abertos.
- **Criação de arquivo** - Ativa ou desativa o rastreamento dos arquivos criados ou modificados recentemente.
- **Execução de arquivo** - Ativa ou desativa o rastreamento de arquivos executados.
- **Acesso à mídia removível** - Ativa ou desativa o rastreamento disparado ao acessar mídia removível em particular com espaço de armazenamento.

4.1.1.1.1 Opções de rastreamento avançadas

Opções de configuração mais detalhadas podem ser encontradas em **Computador** > **Antivírus e antispyware** > **Proteção do sistema em tempo real** > **Configuração avançada**.

Parâmetros ThreatSense adicionais para arquivos criados e modificados recentemente - A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior do que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, é usada a heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do banco de dados de assinatura de vírus. Além dos arquivos recém-criados, o rastreamento também é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desmarque a opção **Configurações padrão de rastreamento em arquivos compactados**.

Parâmetros ThreatSense adicionais para arquivos executados - Por padrão, a heurística avançada não é usada quando os arquivos são executados. Entretanto, em alguns casos pode ser necessário ativar essa opção (marcando a opção **Heurística avançada na execução de arquivos**). Observe que a heurística avançada pode tornar mais lenta a execução de alguns programas devido ao aumento dos requisitos do sistema. Enquanto a opção **Heurística avançada na execução de arquivos da mídia removível** estiver ativada, se você desejar excluir algumas portas (USB) de mídia removível de serem rastreadas pela heurística avançada na execução do arquivo, clique em **Exceções...** para abrir a janela de exclusões da unidade de mídia removível. Nessa janela, você poderá personalizar as configurações marcando ou desmarcando as caixas de seleção que representam cada porta.

4.1.1.1.2 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar, clique em **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e clique em **Limpeza**).

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza padrão - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

4.1.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver um conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

Após a instalação do ESET NOD32 Antivirus, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada** > **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos**).

4.1.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo está disponível para download em http://www.eicar.org/download/eicar.com

4.1.1.1.5 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** na janela principal do programa e clique em **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está desativada. Para ativar essa opção, navegue até Configuração avançada (F5) e clique em **Computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, certifique-se de que a caixa de seleção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está marcada.

Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema antes da instalação da ESET.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativada a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Se for este o caso, entre em contato com o Atendimento ao Cliente da ESET.

4.1.1.2 Rastrear o computador

O rastreador sob demanda é uma parte importante da sua solução antivírus. Ele é usado para realizar rastreamentos nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema para detectar vírus que não tenham sido capturados pela Proteção em tempo real do sistema de arquivos quando foram gravados no disco. Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o banco de dados de vírus for obsoleto ou se o arquivo não for detectado como vírus ao ser salvo no disco.

Há dois tipos de **Rastrear o computador** disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastrear o computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem do Rastreamento inteligente é que ele é fácil de operar e não requer configuração de rastreamento detalhada. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza.

Rastreamento personalizado

O rastreamento personalizado permite especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Rastreamento de mídia removível

Semelhante ao rastreamento inteligente - inicie rapidamente um rastreamento de mídia removível (como CD/DVD/USB) atualmente conectada ao computador. Isso pode ser útil quando você conectar uma unidade flash USB a um computador e quiser rastrear seu conteúdo quanto a malware e ameaças em potencial.

Esse tipo de rastreamento também pode ser iniciado clicando em **Rastreamento personalizado** e selecionando **Mídia removível** no menu suspenso **Alvos de rastreamento** e clicando em **Rastrear**.

Leia Progresso do rastreamento para obter mais informações sobre o processo de rastreamento.

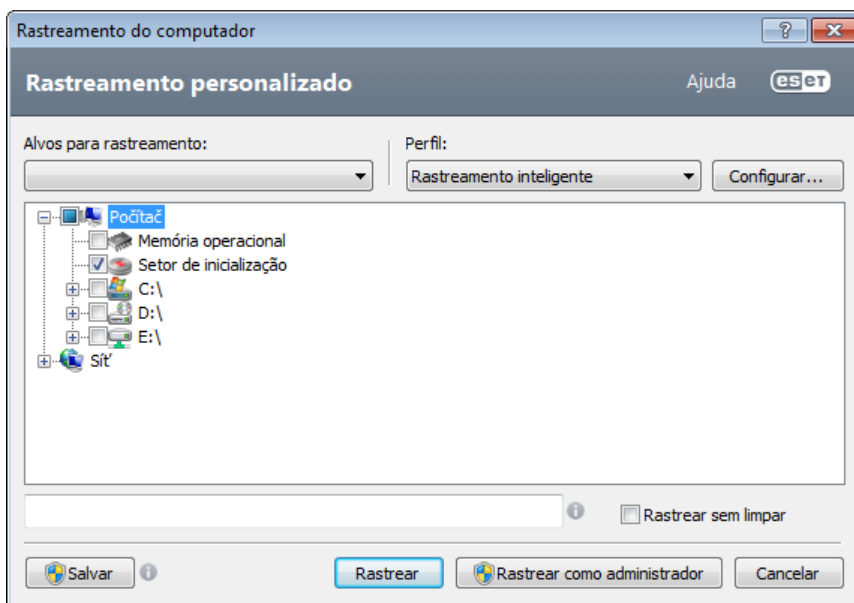
Recomendamos que execute um rastrear o computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

4.1.1.2.1 Iniciador de rastreamento personalizado

Se desejar não verificar o espaço de disco inteiro, mas somente um alvo específico, você poderá usar a ferramenta Rastreamento personalizado clicando em **Rastrear o computador** > **Rastreamento personalizado** e selecionar uma opção no menu suspenso **Alvos de rastreamento** ou selecionar alvos específicos na estrutura de pasta (em árvore).

A janela Alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Nenhuma seleção** - Cancela todas as seleções.

Para navegar rapidamente até um alvo de rastreamento selecionado ou para adicionar diretamente um alvo desejado (pasta ou arquivo(s)), digite-o no campo em branco embaixo da lista de pastas. Isso só é possível se nenhum alvo tiver sido selecionado na estrutura em árvore e se o menu **Alvos de rastreamento** estiver definido como **Nenhuma seleção**.

Os itens infectados não são limpos automaticamente. O rastreamento sem limpar pode ser usado para obter uma visão geral do status de proteção atual. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**. As informações sobre o rastreamento serão salvas em um relatório de rastreamento.

Você pode escolher um perfil no menu suspenso **Perfil de rastreamento** para ser usado para rastreamento dos alvos escolhidos. O perfil padrão é **Rastreamento inteligente**. Há mais dois perfis de rastreamento predefinidos intitulados **Rastreamento detalhado** e **Rastreamento do menu de contexto**. As diferenças entre esses perfis de rastreamento estão no uso de diferentes parâmetros do mecanismo ThreatSense durante o rastreamento de um computador. Clique no botão **Configuração...** para configurar em detalhes o perfil de rastreamento escolhido no menu Perfil de rastreamento. As opções disponíveis são descritas em Configuração do scanner.

Use o botão **Salvar**, que salva as alterações feitas na seleção de alvos, incluindo seleções feitas dentro da estrutura em árvore da pasta.

Clique em **Rastrear** para executar o rastreamento com os parâmetros personalizados definidos.

O botão **Rastrear como administrador** permite que você execute o rastreamento usando a conta do administrador. Clique nessa opção se o usuário que estiver conectado neste momento não tiver privilégios suficientes para acessar os arquivos apropriados para serem rastreados. Observe que esse botão não estará disponível se o usuário atualmente conectado não puder acionar operações de UAC como Administrador.

4.1.1.2.2 Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.

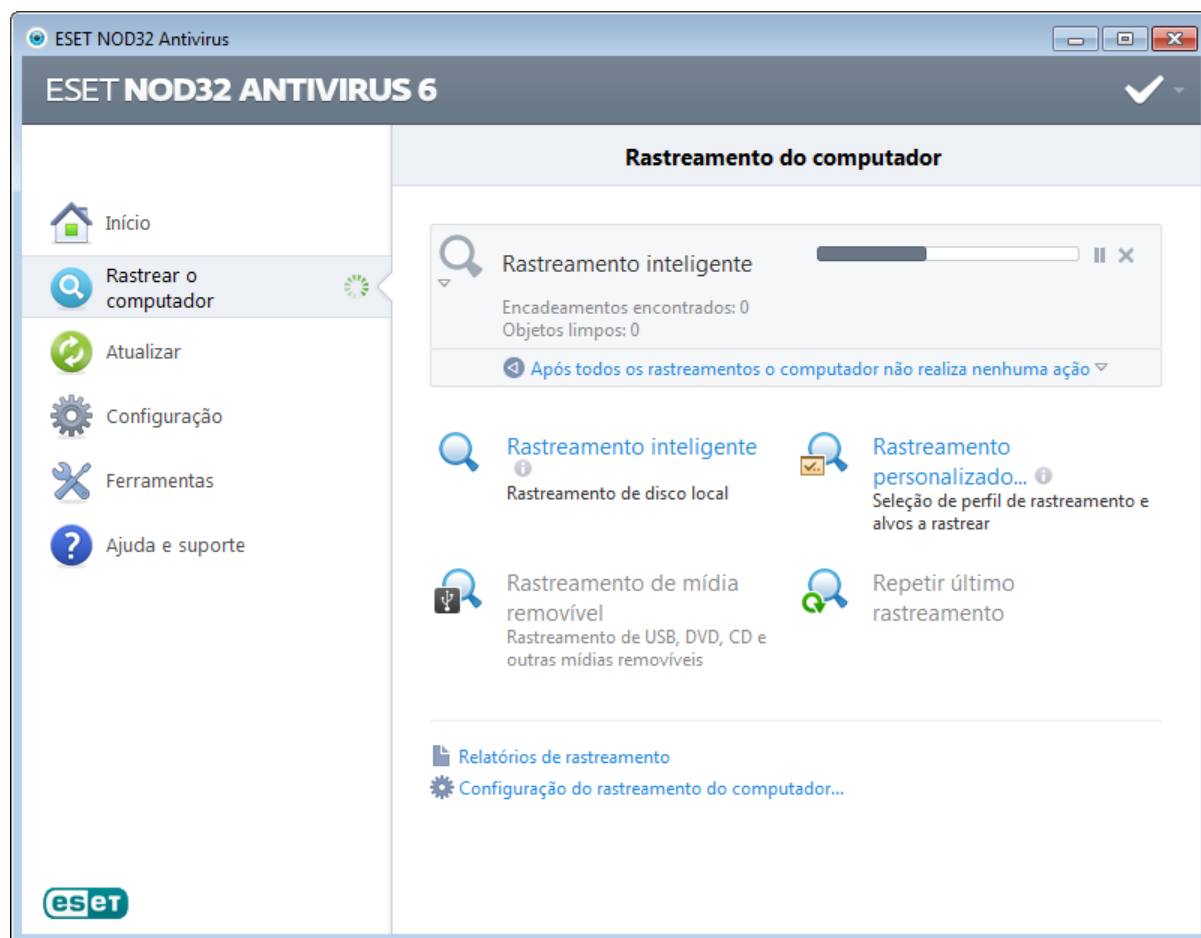
OBSERVAÇÃO: É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente *pagefile.sys* e determinados arquivos de log), não possam ser rastreados.

A barra de progresso mostra o percentual de objetos já rastreados em relação aos objetos ainda aguardando para serem rastreados. Esse valor é derivado do número total de objetos incluídos em um rastreamento.

Dicas

Clique na lupa ou seta para mostrar detalhes sobre o rastreamento que está atualmente em execução.
Você pode executar outro rastreamento paralelo clicando em **Rastreamento inteligente** ou **Rastreamento personalizado...**.

Objetos - Mostra o número total de arquivos rastreados, ameaças encontradas e ameaças limpas durante um rastreamento.

Destino - O nome do objeto rastreado no momento e sua localização.

Após todos os rastreamentos o computador não realizará nenhuma ação - Permite que você crie uma reinicialização ou desligamento agendado quando o computador concluir o rastreamento. Assim que o rastreamento for concluído, uma janela de diálogo de confirmação do desligamento aparecerá e permanecerá aberta por 60 segundos. Clique nessa opção novamente para desativar a ação selecionada.

4.1.1.2.3 Perfis de rastreamento

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Computador** > **Antivírus e antispyware** > **Rastrear o computador** > **Perfis...**. A janela **Perfis de configuração** inclui o menu suspenso **Perfil selecionado** que lista os perfis de rastreamento existentes e a opção para criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Digite o nome do novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil**. Depois, ajuste os demais parâmetros de maneira a atender as suas necessidades.

4.1.1.3 Rastreamento na inicialização

O rastreamento automático de arquivo na inicialização será executado na inicialização do sistema ou durante a atualização do banco de dados de assinatura de vírus. Esse rastreamento depende das Tarefas e configurações da agenda.

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para alterar suas configurações, acesse **Ferramentas** > **Agenda**, clique em **Rastreamento automático de arquivo na inicialização** e no botão **Editar...**. Na última etapa, a janela Rastreamento automático de arquivo na inicialização será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte Criação de novas tarefas.

4.1.1.3.1 Rastreamento de arquivos em execução durante inicialização do sistema

Ao criar uma tarefa agendada de Rastreamento de arquivo na inicialização do sistema, você tem várias opções para ajustar os seguintes parâmetros:

O menu suspenso **Nível de rastreamento** especifica a profundidade do rastreamento da execução de arquivos na inicialização do sistema. Os arquivos são organizados em ordem crescente de acordo com os seguintes critérios:

- **Somente os arquivos usados com mais frequência** (menos arquivos rastreados)
- **Arquivos usados com frequência**
- **Arquivos usados comumente**
- **Arquivos usados raramente**
- **Todos os arquivos registrados** (mais arquivos rastreados)

Dois grupos específicos de **Nível de rastreamento** também estão inclusos:

- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que podem ser acessados sem que o usuário esteja conectado (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que podem ser acessados após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

As listas de arquivos a serem rastreados estão fixas para cada grupo anteriormente.

Prioridade do rastreamento - O nível de prioridade usado para determinar quando um rastreamento iniciará:

- **Normal** - em uma carga média do sistema,
- **Baixa** - em uma carga baixa do sistema,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera.

4.1.1.4 Rastreamento em estado ocioso

O rastreamento em estado ocioso pode ser configurado e ativado em **Configuração avançada**, em **Computador** > **Antivírus e antispyware** > **Rastreamento em estado ocioso**. Quando o computador estiver em estado ocioso, então um rastreamento sem segundo plano do computador será realizado em todas as unidades locais. Consulte também acionadores de detecção no estado ocioso (p. ex., proteção de tela, logoff de usuário), que devem ser atendidos para executar o rastreamento no estado ocioso.

Por padrão, o rastreamento no estado ocioso não será executado quando o computador (notebook) estiver sem bateria e não estiver conectado à tomada. No entanto, aqui, você pode substituir essa exceção.

Clique em **Ativar registro em log** para ver o resultado da verificação do computador na seção Arquivos de log (na janela do programa principal, clique em **Ferramentas** > **Arquivos de log** e, no menu suspenso **Log**, escolha **Rastrear o computador**).

A última configuração aqui é Configuração de parâmetros do mecanismo ThreatSense. Clique em **Configuração...** se você quiser modificar vários parâmetros de verificação (p. ex., métodos de detecção).

4.1.1.5 Exclusões

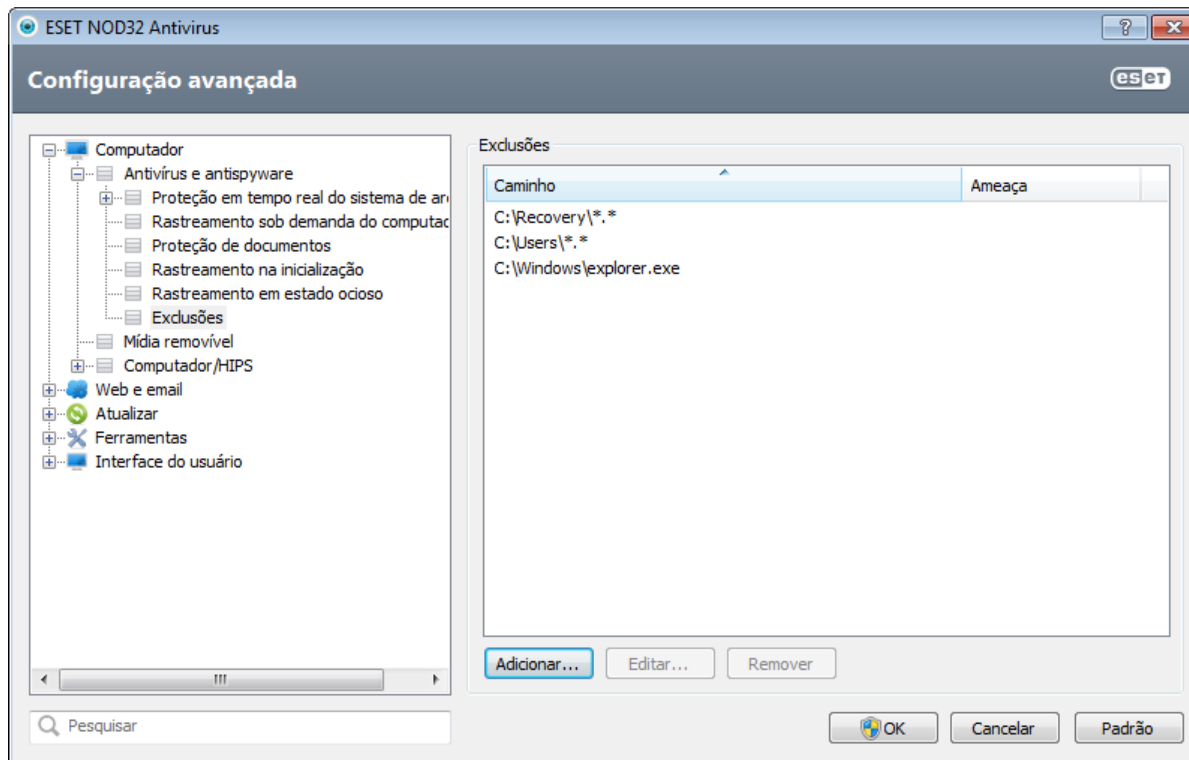
As exclusões permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exceções somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Entretanto, existem situações em que você precisará excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação.

Para excluir um objeto do rastreamento:

1. Clique em **Adicionar...**,
2. Digite o caminho para um objeto ou selecione-o na estrutura em árvore.

Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

Exemplos

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara “*.*”.
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara “*.doc”.
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, “D”), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).

Observação: uma ameaça em um arquivo não será detectada pelo módulo de proteção em tempo real do sistema de arquivos ou módulo de rastreamento do computador se um arquivo atender aos critérios para exclusão do rastreamento.

Caminho - caminho para arquivos e pastas excluídos.

Ameaça - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, e não completamente. Se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus. Esse tipo de exclusão pode ser utilizado apenas para determinados tipos de infiltrações e pode ser criado na janela de alerta de ameaças que informa a infiltração (clique em **Mostrar opções avançadas** e selecione **Excluir da detecção**) ou clicando em **Configuração** > **Quarentena**, clicando com o botão direito do mouse no arquivo em quarentena e selecionando **Restaurar e excluir da detecção** no menu de contexto.

Adicionar... - exclui objetos da detecção.

Editar... - permite que você edite as entradas selecionadas.

Remover - remove as entradas selecionadas.

4.1.1.6 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é a tecnologia que consiste em muitos métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante a propagação inicial de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados.
- A combinação de diversos métodos de detecção.
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos,
- Proteção de documentos,
- Proteção do cliente de email,
- Proteção do acesso à web,
- Rastrear o computador.

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastrear o computador.

4.1.1.6.1 Objetos

A seção **Objetos** permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

Memória operacional - Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização - Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

Arquivos de email - O programa oferece suporte às seguintes extensões: DBX (Outlook Express) e EML.

Arquivos compactados - O programa oferece suporte às seguintes extensões: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e muitas outras.

Arquivos compactados de autoextração - Os arquivos compactados de auto-extração (SFX, Self-extracting archives) são arquivos compactados que não requerem programas especializados - arquivos compactados - para se descompactarem.

Empacotadores em tempo real - Depois da execução, os empacotadores em tempo real (ao contrário dos arquivos compactados padrão) fazem a descompactação na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o scanner é compatível (graças à emulação do código) com muitos mais tipos de empacotadores.

4.1.1.6.2 Opções

Na seção **Opções**, é possível selecionar os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

Heurística - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal vantagem é a capacidade de identificar software malicioso que não existia ou que não era identificado pelos bancos de dados das assinaturas de vírus anteriores. A desvantagem é uma probabilidade pequena de alarmes falsos.

Heurística avançada/DNA/Assinaturas inteligentes - A heurística avançada consiste em um algoritmo de heurística exclusivo desenvolvido pela ESET, otimizado para detecção de worms e cavalos de troia no computador e escrito em linguagens de programação de alto nível. Graças à heurística avançada, a capacidade de detecção do programa é significativamente superior. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

ESET Live Grid - Graças à tecnologia de reputação da ESET, as informações sobre os arquivos rastreados são verificadas em relação aos dados do ESET Live Grid baseado na nuvem , a fim de melhorar a detecção e a velocidade de rastreamento.

4.1.1.6.3 Limpeza

As configurações de limpeza determinam o comportamento do scanner enquanto limpa os arquivos infectados. Há três níveis de limpeza:

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza padrão - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

4.1.1.6.4 Extensões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** estiver desmarcada, a lista será alterada para exibir todas as extensões de arquivos rastreados no momento.

Para habilitar o rastreamento de arquivos sem uma extensão, selecione a opção **Rastrear arquivos sem extensão**. A opção **Não rastrear arquivos sem extensão** é disponibilizada quando a opção **Rastrear todos os arquivos** é ativada.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando as extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

Com os botões **Adicionar** e **Remover**, você pode autorizar ou proibir o rastreamento de extensões de arquivos específicas. Digitar uma **Extensão** ativa o botão **Adicionar**, que adiciona a nova extensão à lista. Selecione uma extensão na lista e, em seguida, clique no botão **Remover** para excluir essa extensão da lista.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista.

Para rastrear somente o conjunto padrão de extensões, clique em **Padrão** e clique em **Sim**, quando solicitado, para confirmar.

4.1.1.6.5 Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Tamanho máximo do objeto - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento. Valor padrão: *sem limite*.

Tempo máximo do rastreamento para objecto (s) - Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento. Valor padrão: *sem limite*.

Nível de compactação de arquivos compactados - Especifica a profundidade máxima do rastreamento de arquivos compactados. Valor padrão: *10*.

Tamanho máximo do arquivo no arquivo compactado - Essa opção permite especificar o tamanho máximo de arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Valor padrão: *sem limite*.

Se o rastreamento de um arquivo compactado for encerrado prematuramente por essa razão, o arquivo compactado permanecerá desmarcado.

Observação: Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

4.1.1.6.6 Outros

Na seção **Outros**, é possível configurar as seguintes opções:

Registrar todos os objetos - Se essa opção estiver selecionada, o arquivo de log mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados. Por exemplo, se uma infiltração for encontrada dentro de um arquivo compactado, o log também listará os arquivos limpos contidos dentro do arquivo compactado.

Ativar otimização inteligente - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento do computador, as seguintes opções também estarão disponíveis:

Rastrear fluxos dados alternativos (ADS) - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade - Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

Manter último registro de acesso - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Percorrer log de rastreamento - Essa opção permite ativar/desativar o rolamento do log. Se selecionada, as informações rolam para cima dentro da janela de exibição.

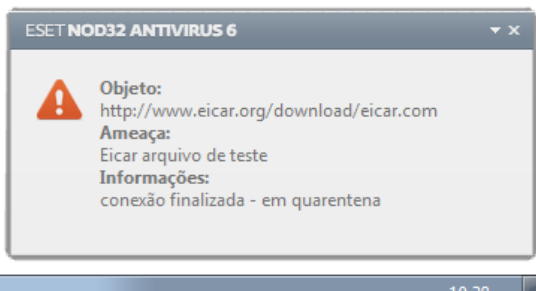
4.1.1.7 Uma infiltração foi detectada

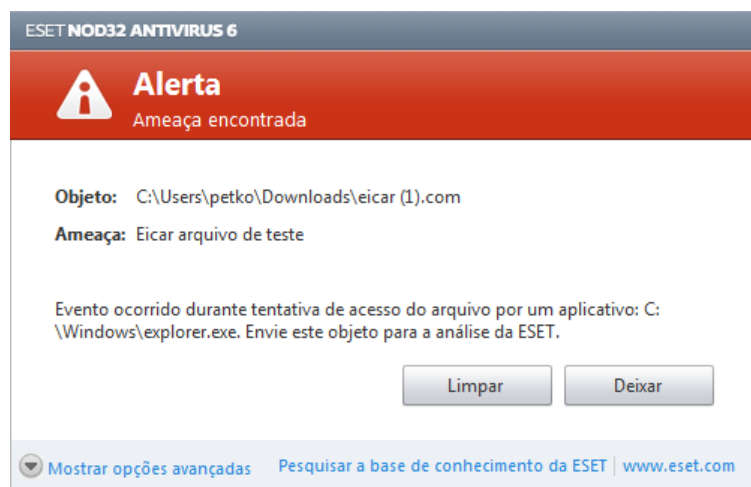
As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como páginas da web, pastas compartilhadas, via email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET NOD32 Antivirus, as infiltrações podem ser detectadas usando

- Proteção em tempo real do sistema de arquivos,
- Proteção do acesso à web,
- Proteção do cliente de email ou
- Rastreamento sob demanda do computador,

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a Quarentena ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para obter mais informações sobre níveis de limpeza e de comportamento, consulte Limpeza.

Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.

Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Várias ameaças

Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o nível de limpeza estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione as ações adequadas para esses arquivos. Selecione ações para os arquivos (as ações são definidas individualmente para cada arquivo na lista) e clique em **Finalizar**.

Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza ativado o arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET NOD32 Antivirus e clique em Rastrear o computador.
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte Rastreamento de computador),
- Após a conclusão do rastreamento, revise o log para obter informações como o número de arquivos rastreados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

4.1.1.8 Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. A proteção de documentos fornece uma camada de proteção além da proteção do sistema de arquivos em tempo real, bem como pode ser desativada para aprimorar o desempenho em sistemas não expostos a um alto volume de documentos do Microsoft Office.

Integrar ao sistema ativa o sistema de proteção. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Compuador** > **Antivírus e antispyware** > **Proteção de documentos** na árvore Configuração avançada. Quando ativada, a Proteção de documentos pode ser visualizada na janela principal do ESET NOD32 Antivirus em **Configuração** > **Computador**.

Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

4.1.2 Mídia removível

O ESET NOD32 Antivirus fornece controle automático de mídia removível (CD/DVD/USB/...). Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e seleciona como o usuário pode acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

Mídia removível compatível

- CD/DVD/Blu-ray
- Chave USB
- Unidade USB
- FireWire

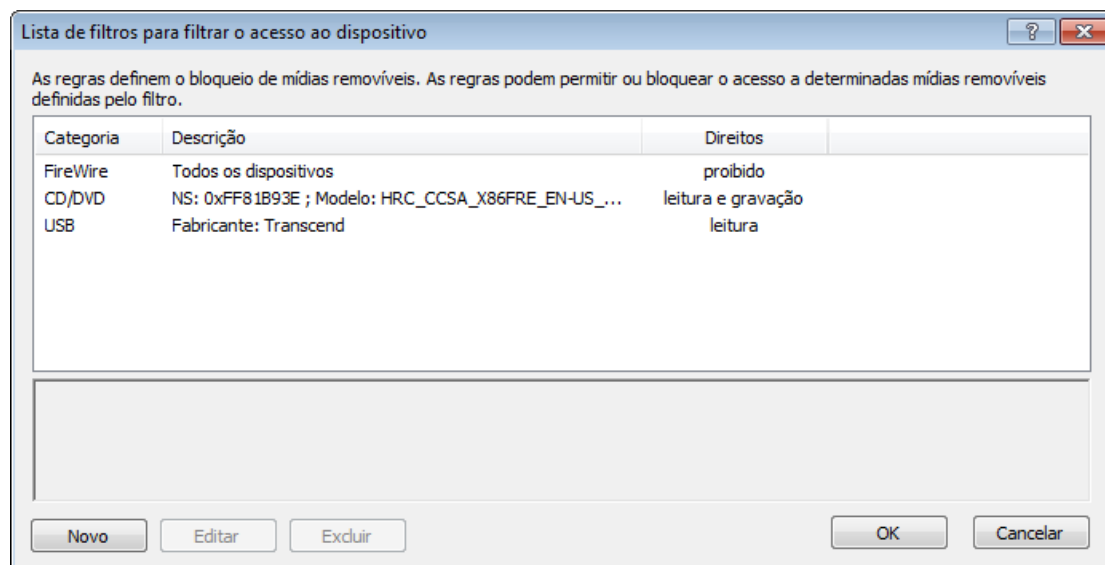
Ação a ser executada após inserção da mídia removível - Selecione a ação padrão que será desenvolvida quando um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Se a opção **Mostrar opções de rastreamento** for selecionada, será exibida uma notificação que lhe permite selecionar a ação desejada:

- **Rastrear agora** - Um rastreamento do computador sob demanda do dispositivo de mídia removível inserido será executado.
- **Rastrear mais tarde** - Nenhuma ação será executada e a janela **Novo dispositivo detectado** será fechada.
- **Configurar...** - Abre a seção de configuração da mídia removível.

Regras de bloqueio de mídia removível - Selecione essa opção para bloquear toda a mídia removível conectada ao computador. Se desejar que algumas mídias permaneçam disponíveis, exclua-as do bloqueio.

Clique em **Regras...** para permitir ou bloquear o acesso à mídia removível selecionada. É possível gerenciar as regras estendidas para a mídia removível nessa janela. As regras podem ser filtradas pelo tamanho da mídia, pelo número serial e pelo tipo de dispositivo. Cada regra tem suas próprias permissões, portanto, você pode permitir, limitar ou bloquear o acesso à mídia removível selecionada. Mais detalhes sobre rastreamento e bloqueio de mídia removível podem ser encontrados no capítulo Editar regra de filtragem.

4.1.2.1 Regras de filtragem

A janela Filtrar acesso ao dispositivo exibe as regras estendidas existentes para a mídia removível.

Categoria - Tipo de mídia removível (CD/DVD/USB...).

Descrição - Descrição das regras de filtro para o dispositivo.

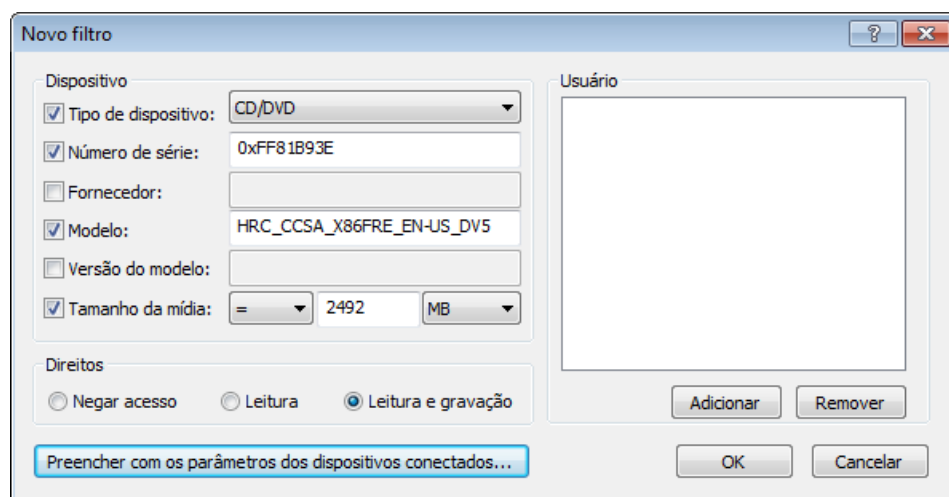
Direitos - Permissões associadas de determinados dispositivos, que correspondem aos critérios definidos pelo filtro.

Nova - Crie uma nova regra de filtro para mídia removível.

Editar - Selecione uma linha e clique nesse botão para alterar a regra existente.

Excluir (Del) - Remova a regra selecionada.

4.1.2.2 Editar regra de filtragem

Para adicionar ou editar uma regra de filtragem existente, clique em **Novo** ou **Editar** na janela Filtrar acesso ao dispositivo. As opções e configurações de dispositivo a seguir estão disponíveis na janela Filtrar acesso ao dispositivo.

Dispositivo

- **Tipo de dispositivo** - Escolha o tipo de mídia removível na lista (CD/DVD/USB).
- **Número de série** - Uma mídia removível geralmente tem seu próprio número de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.
- **Fornecedor** - Filtragem por nome ou ID do fornecedor.
- **Modelo** - O nome dado ao dispositivo (geralmente escolhido pelo proprietário ou fornecedor).
- **Versão do modelo** - A versão do dispositivo específico, se disponível (opcional).
- **Tamanho da mídia** - Ao ativar essa opção você pode definir os dispositivos de filtro condicional (maior que, igual a, menor que) pelo tamanho da mídia (bytes, megabytes etc.).

Observação: Os parâmetros de filtragem em todos os campos de texto fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são suportados. Eles precisam ser gravados exatamente como entregues pelo fornecedor. Clique na opção **Preencher com os parâmetros dos dispositivos conectados...** para escolher/preencher com os parâmetros de dispositivo de mídia removível para dispositivos conectados ao seu computador.

Direitos

- **Negar acesso** - O acesso ao dispositivo não será concedido. Uma janela com informações de bloqueio do dispositivo será exibida quando uma tentativa de acesso ao dispositivo for realizada.
- **Leitura** - O usuário pode ler os arquivos de uma mídia removível.
- **Leitura e gravação** - Total controle sobre a mídia removível.

Usuário

- **Adicionar** - Abre a janela de diálogo **Tipo de objeto: Usuários ou Grupos** que permite a seleção dos usuários desejados.
- **Remover** - Remove o usuário selecionado do filtro.

4.1.3 Sistema de prevenção de intrusos de host (HIPS)

O **Sistema de prevenção de intrusos de host** (HIPS) protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

O HIPS pode ser encontrado em **Configuração avançada** (F5) clicando em **Computador** > **HIPS**. O status do HIPS (ativado/desativado) é exibido na janela principal do ESET NOD32 Antivirus, no painel **Configuração**, à direita da seção **Computador**.

As configurações do HIPS estão localizadas na **Configuração avançada** (F5). Para acessar o HIPS, na árvore Configuração avançada, clique em **Computador** > **HIPS**. O status do HIPS (ativado/desativado) é exibido na janela principal do ESET NOD32 Antivirus, no painel **Configuração**, à direita da seção Computador.

Aviso: apenas um usuário experiente deve fazer alterações nas configurações do HIPS.

O ESET NOD32 Antivirus tem uma tecnologia de *Autodefesa* incorporada que impede que o software malicioso danifique ou desabilite a proteção antivírus e anti-spyware.

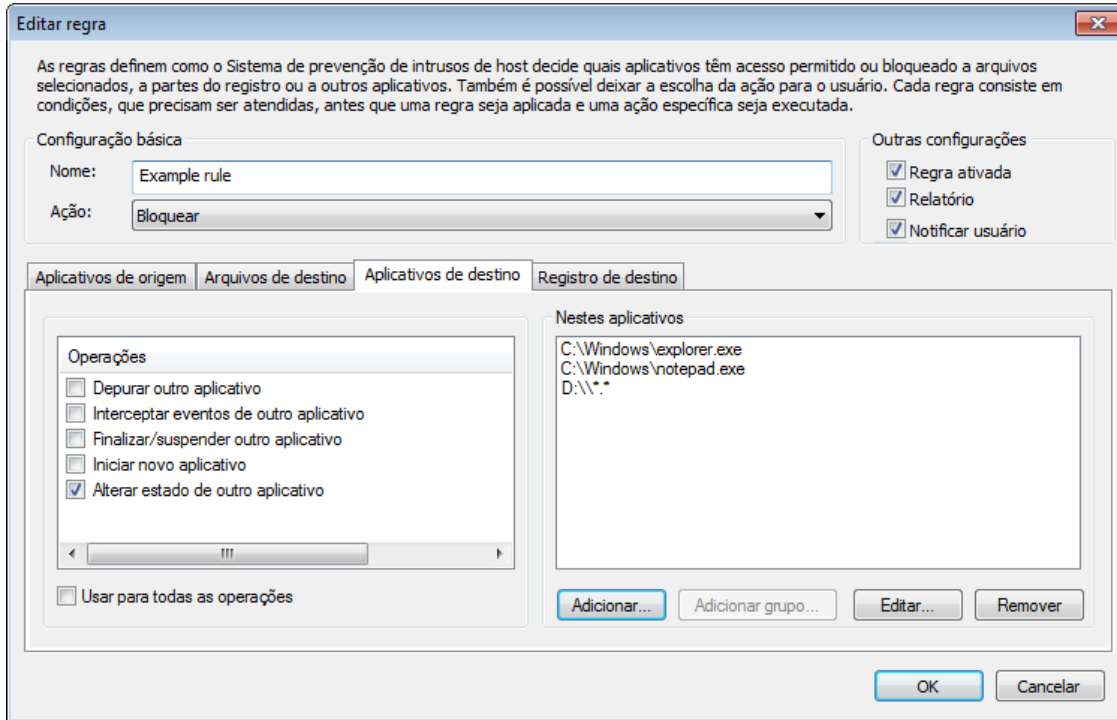
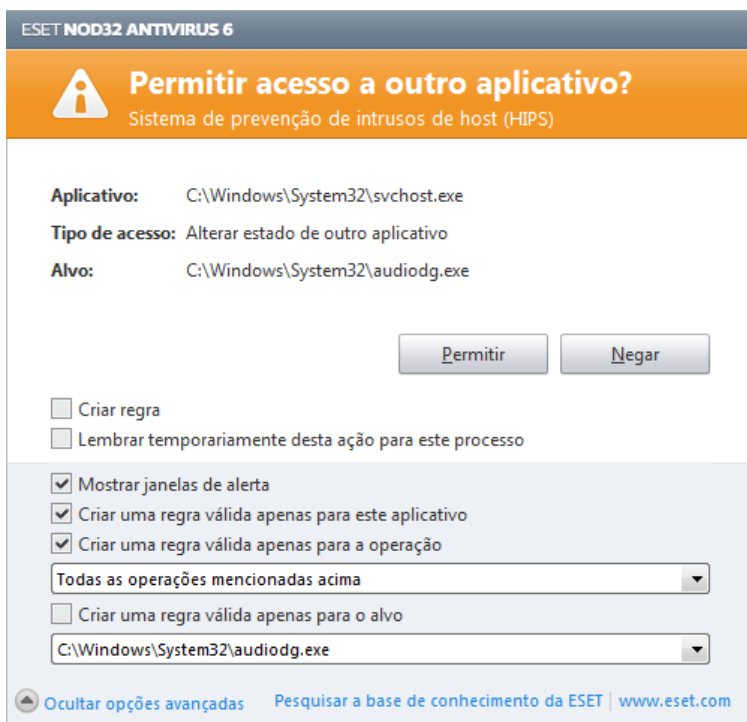
As alterações executadas nas configurações **Ativar HIPS** e **Ativar autodefesa** entram em vigor depois que o sistema operacional Windows é reiniciado. A desativação de todo o sistema **HIPS** também exigirá uma reinicialização do computador para ser implementada.

A filtragem pode ser executada em um de quatro modos:

- **Modo automático com regras** - As operações são ativadas, exceto as regras predefinidas que protegem o sistema.
- **Modo interativo** - O sistema solicitará que o usuário confirme as operações.
- **Modo com base em políticas** - Operações não definidas por uma regra podem ser bloqueadas.
- **Modo de aprendizagem** - As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no **Editor de regras**, mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Depois de selecionar **Modo de aprendizagem**, a opção**Notificar sobre a expiração do modo de aprendizagem em X dias** fica ativa. Ao término desse período, o modo de aprendizagem será desativado novamente. O prazo máximo é de 14 dias. Ao término desse período, uma janela pop-up será aberta e você poderá editar as regras e selecionar outro modo de filtragem.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares às regras usadas no firewall pessoal. Clique em **Configurar regras...** para abrir a janela de gerenciamento de regras do HIPS. Aqui é possível selecionar, criar, editar ou excluir regras.

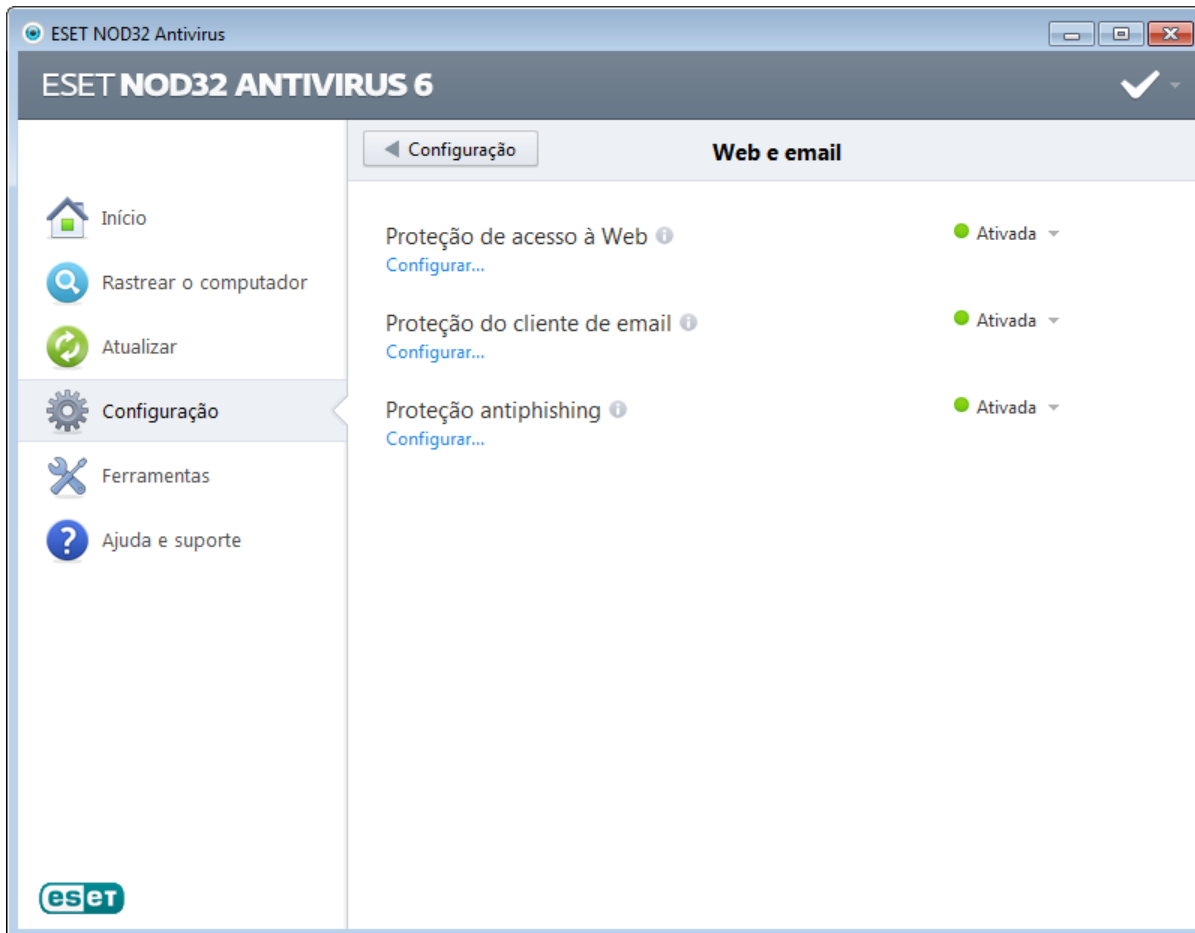
No exemplo a seguir demonstraremos como restringir o comportamento indesejado de aplicativos:

1. Nomeie a regra e selecione **Bloquear** no menu suspenso **Ação**.
2. Abra a guia **Aplicativos de destino**. Deixe a guia **Aplicativos de origem** em branco para que a nova regra seja aplicada a todos os aplicativos tentando realizar qualquer das operações verificadas na lista **Operações** nos aplicativos na lista **Nestes aplicativos**.
3. Selecione **Alterar estado de outro aplicativo** (todas as operações são descritas na ajuda do produto, que pode ser acessada pressionando F1).
4. **Adicione** um ou vários aplicativos que deseja proteger.
5. Marque a caixa de seleção **Notificar usuário** para exibir uma notificação sempre que uma regra for aplicada.
6. Clique em **OK** para salvar a nova regra.

Uma janela de diálogo será exibida sempre que **Perguntar** for a ação padrão. Ela permite que o usuário escolha se deseja **Negar** ou **Permitir** a operação. Se o usuário não definir uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

A janela da caixa de diálogo permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então definirá as condições nas quais permitir ou negar essa ação. Os parâmetros exatos podem ser definidos depois de clicar em **Mostrar opções**. As regras criadas como esta são consideradas iguais às regras criadas manualmente, portanto a regra criada a partir de uma janela de diálogo pode ser menos específica que a regra que acionou a janela de

diálogo. Isso significa que após a criação dessa regra, a mesma operação pode acionar a mesma janela.

A opção **Lembrar temporariamente desta ação para este processo** faz com que a ação (**Permitir**/**Negar**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem seja ativado ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

4.2 Web e email

A configuração da Web e de email pode ser encontrada no painel **Configuração** ao clicar em **Web e email**. A partir daqui, você pode acessar mais configurações detalhadas do programa..

A conectividade com a Internet é um recurso padrão em computadores pessoais. Infelizmente, a Internet tornou-se o meio principal de distribuição de códigos maliciosos. Por esse motivo, é essencial refletir com atenção sobre as suas configurações de **Proteção do acesso à Web**.

A **Proteção do cliente de email** fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP. Usando o plug-in do cliente de email, o ESET NOD32 Antivirus permite controlar todas as comunicações enviadas e recebidas através do cliente de email (POP3, MAPI, IMAP, HTTP).

É possível desativar o módulo de proteção web/email temporariamente clicando em **Ativado**.

Configurar ... - Abre as configurações avançadas da proteção de web/email .

4.2.1 Proteção do cliente de email

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Usando o plug-in para Microsoft Outlook e outros clientes de email, o ESET NOD32 Antivirus permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado oferecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** > **Web e email** > **Proteção do cliente de email**.

Configuração dos parâmetros do mecanismo ThreatSense - A configuração avançada do scanner de vírus permite configurar alvos do rastreamento, métodos de detecção, etc. Clique em **Configuração...** para exibir a janela de configuração do scanner de vírus detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. É possível selecionar **Acrescentar mensagem de marca nos emails recebidos e lidos**, bem como **Acrescentar mensagens de marca a email enviado**. Não se deve confiar nas mensagens de marca sem questioná-las, pois elas podem ser omitidas em mensagens HTML problemáticas ou podem ser forjadas por alguns vírus. As mensagens de marca podem ser adicionadas a um email recebido e lido ou a um email enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Somente para email infectado** - Somente mensagens contendo software malicioso serão marcadas como rastreadas (padrão).
- **Para todos os emails rastreados** - o programa anexará mensagens a todos os emails rastreados.

Acrescentar observação ao assunto de email infectado recebido e lido/enviado - Marque essa caixa de seleção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples com base em assunto de email infectado (se compatível com o seu programa de email). Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

Modelo adicionado ao assunto de email infectado - Edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado. Essa função substituirá o assunto da mensagem *"Olá"* com o prefixo *"[vírus]"* para o seguinte formato: *"[virus] Olá"*. A variável *%VIRUSNAME%* representa a ameaça detectada.

4.2.1.1 Integração com clientes de email

A integração do ESET NOD32 Antivirus com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET NOD32 Antivirus. Se a integração for ativada, a barra de ferramentas do ESET NOD32 Antivirus será inserida diretamente no cliente de email, permitindo proteção mais eficiente aos emails. As configurações da integração estão disponíveis na seção **Configuração** > **Entrar na configuração avançada...** > **Web e email** > **Proteção do cliente de email** > **Integração com clientes de email**.

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Selecione a caixa de seleção próxima a **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao recuperar emails do Kerio Outlook Connector Store.

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

4.2.1.1.1 Configuração da proteção do cliente de email

O módulo de proteção do cliente de email suporta os seguintes clientes de email: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do controle de plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus.

Email para ser rastreado

Email recebido - Alterna a verificação das mensagens recebidas.
Email enviado - Alterna a verificação das mensagens enviadas.
Email lido - Alterna a verificação das mensagens lidas.

Ação que será executada no email infectado

Nenhuma ação - Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.
Excluir email - O programa notificará o usuário sobre infiltrações e excluirá a mensagem.
Mover email para a pasta Itens excluídos - Os emails infectados serão movidos automaticamente para a pasta **Itens excluídos**.
Mover email para pasta - Especifique a pasta personalizada para a qual você deseja mover o email infectado quando detectado.

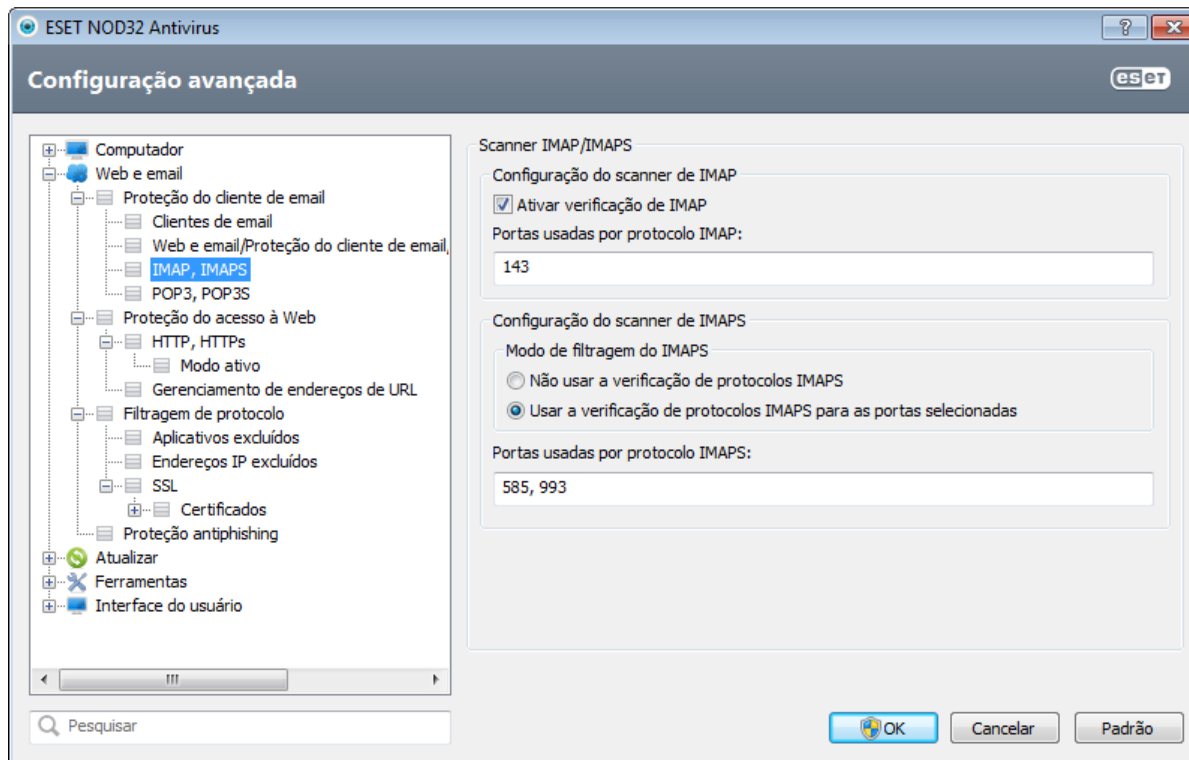
Outros

Repetir o rastreamento após atualização - Alterna o rastreamento depois de uma atualização do banco de dados de assinatura de vírus.
Aceitar resultados de rastreamento de outros módulos - Se essa opção for selecionada, o módulo de proteção do email aceitará os resultados de rastreamento de outros módulos de proteção.

4.2.1.2 Scanner IMAP, IMAPS

O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de emails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de correio e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou excluída. O ESET NOD32 Antivirus fornece proteção para este protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. O controle do protocolo IMAP é feito automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 143 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

4.2.1.3 Filtro POP3, POP3S

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET NOD32 Antivirus fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado - a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

Nesta seção, é possível configurar a verificação dos protocolos POP3 e POP3S.

Ativar verificação do protocolo POP3 - Se estiver ativada, todo o tráfego por meio do POP3 será monitorado quanto a software malicioso.

Portas usadas pelo protocolo POP3 - Uma lista de portas utilizadas pelo protocolo POP3 (110 por padrão).

O ESET NOD32 Antivirus oferece também suporte à verificação do protocolo POP3S. Esse tipo de comunicação utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET NOD32 Antivirus verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte).

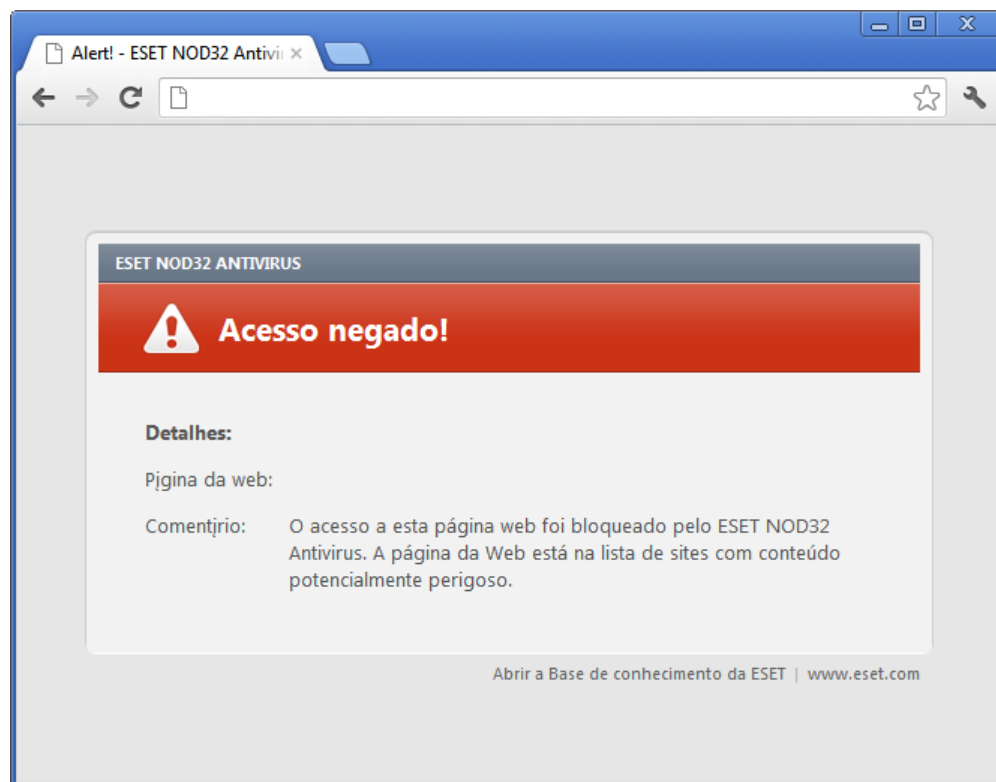
Não utilizar a verificação de POP3S - A comunicação criptografada não será verificada.

Utilizar a verificação de protocolo POP3S para as portas selecionadas - Selecione essa opção para permitir a verificação de POP3S apenas para as portas definidas em **Portas utilizadas pelo protocolo POP3S**.

Portas utilizadas pelo protocolo POP3S - Uma lista de portas POP3S a serem verificadas (por padrão, 995).

4.2.2 Proteção do acesso à Web

A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção de acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPS (comunicação criptografada).

Recomendamos enfaticamente que a proteção de acesso à Web seja ativada. Essa opção pode ser acessada a partir da janela principal do ESET NOD32 Antivirus localizada em **Configuração** > **Web e email** > **Proteção de acesso à Web**. O acesso a páginas da web conhecidas por ter conteúdo malicioso sempre será bloqueado.

4.2.2.1 HTTP, HTTPs

Por padrão, o ESET NOD32 Antivirus está configurado para usar os padrões da maioria dos navegadores de Internet. Contudo, as opções de configuração do scanner HTTP podem ser modificadas em **Configuração avançada** (F5) > **Web e email** > **Proteção do acesso à web** > **HTTP, HTTPS**. Na janela principal **Rastreamento HTTP/HTTPS**, é possível selecionar ou desmarcar a opção **Ativar verificação de HTTP**. Você também pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80 (HTTP), 8080 e 3128 (para servidor Proxy) estão predefinidos.

O ESET NOD32 Antivirus oferece suporte à verificação do protocolo HTTPS. A comunicação HTTPS utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET NOD32 Antivirus verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). A verificação de HTTPS pode ser executada nos seguintes modos:

Não utilizar a verificação de protocolo HTTPS - A comunicação criptografada não será verificada.

Utilizar a verificação de protocolo HTTPS para as portas selecionadas - Verificação de HTTPS apenas para as portas definidas em **Portas utilizadas pelo protocolo HTTPS**.

Utilizar a verificação de protocolo HTTPS para portas selecionadas - O programa só verificará esses aplicativos que são especificados na seção navegadores e que utilizam as portas definidas em **Portas utilizadas pelo protocolo HTTPS** . A porta 443 é definida por padrão.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, navegue até Verificação de protocolo SSL na seção Configuração avançada, clique em **Web e email** > **Filtragem de protocolo** > **SSL** e ative a opção **Sempre rastrear o protocolo SSL**.

4.2.2.1.1 Modo ativo para navegadores da web

O ESET NOD32 Antivirus também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da web.

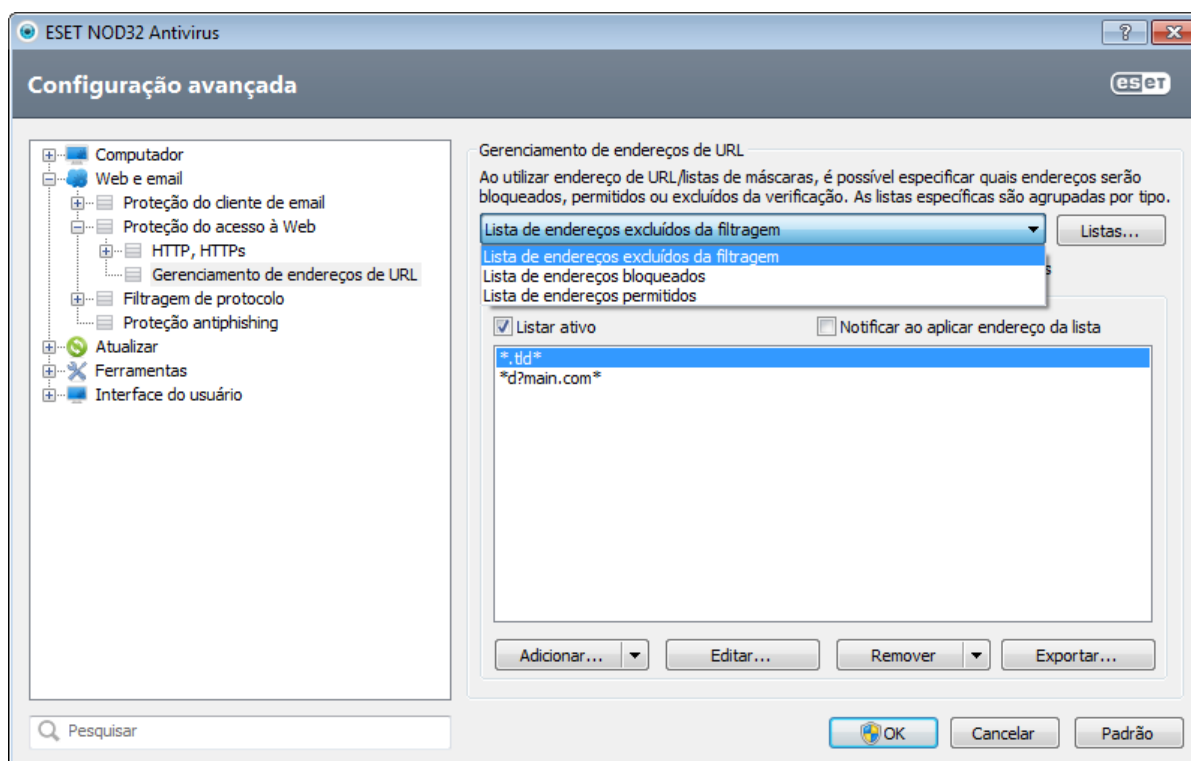
O Modo ativo é útil porque ele examina os dados transferidos de aplicativos acessando a Internet como um todo, independentemente de eles serem marcados como navegadores da web ou não (para obter mais informações, consulte Clientes web e de email). Se o Modo ativo não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece maior compatibilidade para os aplicativos listados. Se nenhum problema ocorrer ao usá-lo, recomendamos que você ative o modo ativo marcando a caixa de seleção ao lado do aplicativo desejado.

O Modo ativo funciona da seguinte forma: quando um aplicativo com acesso à rede fizer download de dados, ele será primeiro salvo em um arquivo temporário criado pelo ESET NOD32 Antivirus. Nesse momento, os dados não estão disponíveis para o aplicativo determinado. Assim que o download for concluído, ele será rastreado contra códigos maliciosos. Se não for encontrada infiltração, os dados serão enviados para o aplicativo original. Esse processo fornece controle completo das comunicações feitas por um aplicativo controlado. Se o modo passivo estiver ativado, os dados serão destinados ao aplicativo original para evitar atingir o tempo limite.

4.2.2.2 Gerenciamento de endereços URL

O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os botões **Adicionar**,**Editar**, **Remover** e **Exportar** são utilizados para gerenciar as listas de endereços. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso. Se você selecionar a opção **Permitir acesso apenas a endereços URL na lista de endereços permitidos**, apenas endereços presentes na lista de endereços permitidos serão acessíveis, enquanto todos os outros endereços HTTP serão bloqueados.

Se você adicionar um endereço URL à **Lista de endereços excluídos da filtragem**, o endereço será excluído do rastreamento. Você também poderá permitir ou bloquear determinados endereços, adicionando-os à **Lista de endereços permitidos** ou **Lista de endereços bloqueados**. Depois de clicar no botão **Listas...**, a janela **Endereço HTTP/ Listas de máscaras** será exibida, na qual poderá **Adicionar** ou **Remover** listas de endereços. Para adicionar endereços de URL de HTTPS à lista, a opção **Sempre rastrear o protocolo SSL** deverá estar selecionada.

Em todas as listas, os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Para ativar uma lista, selecione a opção **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione **Notificar ao aplicar endereço da lista**.

Adicionar.../Do arquivo - Permite adicionar um endereço à lista manualmente (clique em **Adicionar**) ou por meio de um arquivo de texto simples (clique em **Do arquivo**). A opção **Do arquivo** permite adicionar diversos endereços de URL/máscaras salvos em um arquivo de texto.

Editar... - Edite endereços manualmente, por exemplo, adicionando uma máscara ("*" e "?").

Remover/Remover tudo - Clique em **Remover** para excluir os endereços selecionados da lista. Para excluir todos os endereços, selecione **Remover tudo**.

Exportar... - Salve endereços da lista atual em um arquivo de texto simples.

4.2.3 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. O controle funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. Para comunicação criptografada (SSL), consulte **Filtragem de protocolo** > **SSL**.

Integrar ao sistema - Ativa o driver para a funcionalidade de filtragem do protocolo do ESET NOD32 Antivirus.

Ativar filtragem de conteúdo do protocolo de aplicativo - Se ativado, todo o tráfego HTTP(S), POP3(S) e IMAP(S) será verificado pelo rastreamento antivírus.

OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1, o Windows 7 e o Windows Server 2008, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, as seguintes opções não estarão disponíveis:

- **Portas HTTP e POP3** - Limita o roteamento do tráfego ao servidor proxy interno apenas para as portas HTTP e POP3.
- **Aplicativos marcados como navegadores da web e clientes de email** - Limita o roteamento do tráfego para o servidor proxy interno somente para os aplicativos marcados como navegadores e clientes de email (**Web e email** > **Filtragem de protocolo** > **Web e clientes de email**).
- **Portas e aplicativos marcados como navegadores da Internet ou clientes de email** - Ativa o roteamento de todo o tráfego nas portas HTTP e POP3 bem como de toda a comunicação dos aplicativos marcados como navegadores da Internet e clientes de email no servidor proxy interno.

4.2.3.1 Clientes web e de email

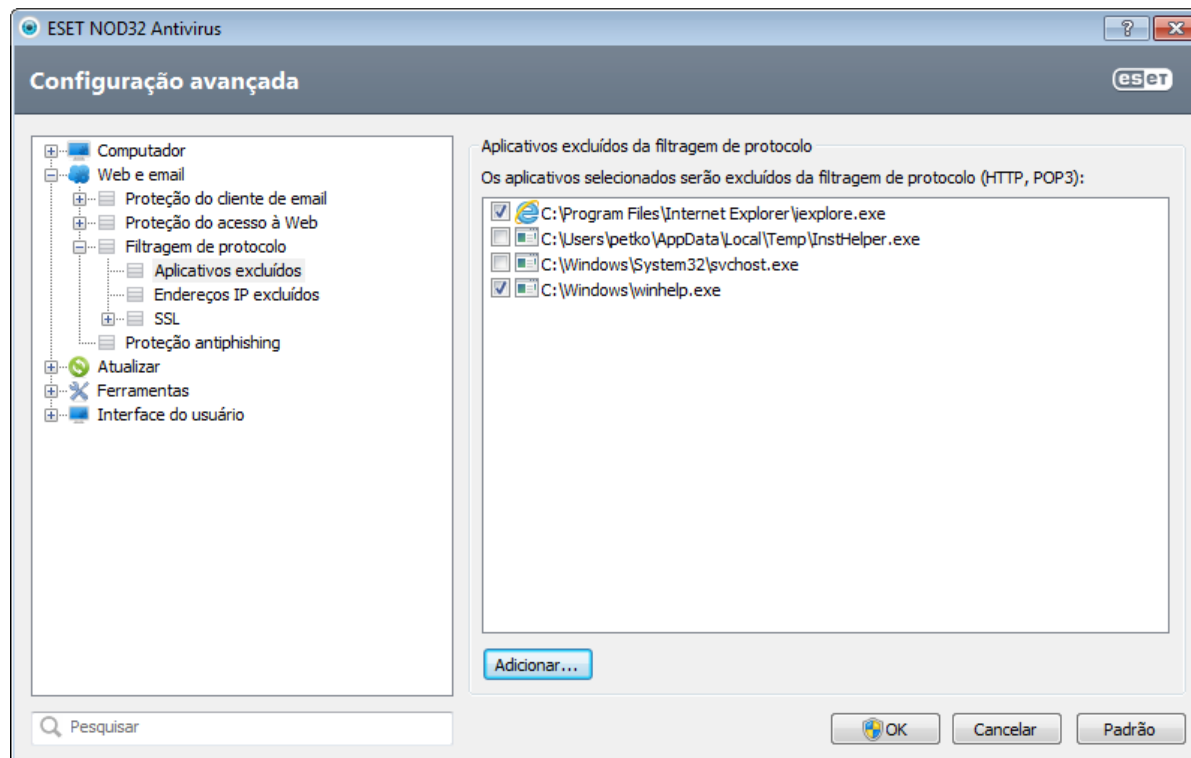
OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, a seção **Clientes web e de email** não está disponível.

Devido à enorme quantidade de códigos maliciosos circulando na Internet, a navegação segura é um aspecto muito importante na proteção do computador. As vulnerabilidades do navegador da Web e os links fraudulentos ajudam o código malicioso a entrar no sistema despercebido e é por isso que o ESET NOD32 Antivirus se focaliza na segurança do navegador da web. Cada aplicativo que acessar a rede pode ser marcado como um navegador da Internet. A caixa de seleção possui dois estados:

- **Desmarcada** - A comunicação de aplicativos é filtrada apenas para as portas especificadas.
- **Marcada** - A comunicação é sempre filtrada (mesmo que uma porta diferente seja definida).

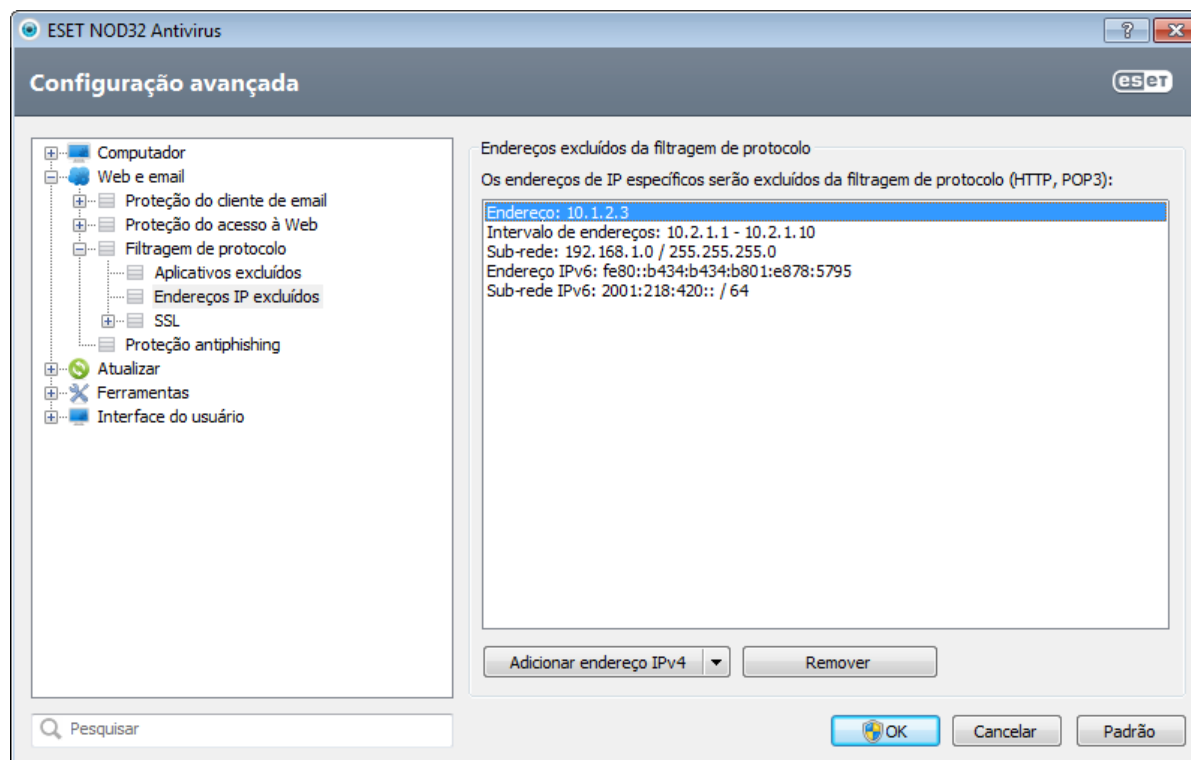
4.2.3.2 Aplicativos excluídos

Para excluir da filtragem de conteúdos a comunicação de aplicativos específicos que possuem direito de acesso à rede, selecione-os na lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção somente para aplicativos que não funcionem corretamente quando a comunicação deles for verificada.

A execução de aplicativos e serviços estará disponível automaticamente. Clique no botão **Adicionar...** para selecionar manualmente um aplicativo não mostrado na lista de filtragem do protocolo.

4.2.3.3 Endereços IP excluídos

As entradas na lista serão excluídas da filtragem de conteúdos do protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços conhecidos como sendo confiáveis.

Adicionar endereço IPv4/IPv6 - Essa opção permite adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra deve ser aplicada.

Remover - Remove as entradas selecionadas da lista.

4.2.3.3.1 Adicionar endereço IPv4

Essa opção permite adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra deve ser aplicada. A versão 4 do IP (Internet Protocol) é a versão mais antiga, mas ainda é a mais amplamente utilizada.

Endereço único - Adiciona o endereço IP de um computador individual para o qual a regra será aplicada (por exemplo, *192.168.0.10*).

Intervalo de endereços - Digite o primeiro e último endereço IP para especificar o intervalo IP (de vários computadores) para o qual a regra será aplicada (por exemplo, *192.168.0.1* a *192.168.0.99*).

Sub-rede - Sub-rede (um grupo de computadores) definida por um endereço IP e máscara.

Por exemplo, *255.255.255.0* é a máscara de rede para o prefixo *192.168.1.0/24*, que significa o intervalo de endereços de *192.168.1.1* a *192.168.1.254*.

4.2.3.3.2 Adicionar endereço IPv6

Essa opção permite adicionar um endereço/sub-rede IPv6 de um ponto remoto para o qual a regra deve ser aplicada. É a versão mais recente do protocolo do IP (Internet Protocol) e substituirá a versão 4 mais antiga.

Endereço único - Adiciona o endereço IP de um computador individual para o qual a regra é aplicada (por exemplo *2001:718:1c01:16:214:22ff:fec9:ca5*).

Sub-rede - A sub-rede (um grupo de computadores) é definida por um endereço IP e máscara (por exemplo: *2002:c0a8:6301:1::1/64*).

4.2.3.4 Verificação do protocolo SSL

O ESET NOD32 Antivirus permite verificar protocolos encapsulados no protocolo SSL. É possível usar vários modos de rastreamento para as comunicações protegidas por SSL utilizando certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Sempre rastrear o protocolo SSL - Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado por você como confiável (ele será adicionado à lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

Perguntar sobre sites não visitados (exclusões podem ser definidas) - Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

Não rastrear o protocolo SSL - Se essa opção estiver selecionada, o programa não rastreará as comunicações em SSL.

Aplicar exceções criadas com base em certificados - Ativa o uso de exclusões especificadas em certificados excluídos e confiáveis para o rastreamento da comunicação SSL. Essa opção estará disponível se você selecionar **Sempre rastrear o protocolo SSL**.

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2 - A comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

4.2.3.4.1 Certificados

Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). Portanto, a opção **Adicionar o certificado raiz a navegadores conhecidos** deve estar ativada. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (ou seja, Opera, Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (ou seja, Internet Explorer). Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (por exemplo, VeriSign). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria das empresas de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se a opção **Perguntar sobre validade do certificado** (padrão) estiver selecionada, o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Uma caixa de diálogo de seleção de ação será exibida, na qual você decidirá marcar o certificado como confiável ou excluído. Se o certificado não estiver presente na lista TRCA, a janela estará vermelha. Se o certificado estiver na lista TRCA, a janela estará verde.

Você poderá selecionar a opção **Bloquear a comunicação que utiliza o certificado** para terminar sempre uma conexão criptografada para o site que usa o certificado não verificado.

Se o certificado não for válido ou estiver corrompido, isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos o bloqueio da comunicação que usa o certificado.

4.2.3.4.1.1 Certificados confiáveis

Além do armazenamento integrado de Autoridades de certificação raiz confiáveis, onde o ESET NOD32 Antivirus armazena os certificados confiáveis, é possível criar uma lista personalizada de certificados confiáveis que pode ser exibida em **Configuração avançada** (F5) > **Web e email** > **Filtragem de protocolo** > **SSL** > **Certificados** > **Certificados confiáveis**. O ESET NOD32 Antivirus verificará o conteúdo da comunicação criptografada utilizando certificados nesta lista.

Para excluir os itens selecionados da lista, clique no botão **Remover**. Clique na opção **Mostrar** (ou clique duas vezes no certificado) para exibir as informações sobre o certificado selecionado.

4.2.3.4.1.2 Certificados excluídos

A seção Certificados excluídos contém certificados que são considerados seguros. O conteúdo das comunicações criptografadas que utilizam os certificados na lista não será verificado com relação a ameaças. Recomendamos excluir apenas os certificados da web que, com certeza, são seguros e a comunicação que utiliza esses certificados não precisa ser verificada. Para excluir os itens selecionados da lista, clique no botão **Remover**. Clique na opção **Mostrar** (ou clique duas vezes no certificado) para exibir as informações sobre o certificado selecionado.

4.2.3.4.1.3 Comunicação SSL criptografada

Se o computador estiver configurado para rastreamento do protocolo SSL, uma janela de diálogo solicitando que você escolha uma ação pode ser aberta quando houver uma tentativa de estabelecer uma comunicação criptografada (utilizando um certificado desconhecido). A janela de diálogo contém as seguintes informações: o nome do aplicativo que iniciou a comunicação e o nome do certificado utilizado.

Se o certificado não estiver localizado no armazenamento de Autoridades de certificação raiz confiáveis, ele será considerado não confiável.

As seguintes ações estão disponíveis para certificados:

Sim - O certificado será marcado temporariamente como confiável para a sessão atual - a janela de alerta não será exibida na próxima tentativa de usar o certificado.

Sim, sempre - Marca o certificado como confiável e adiciona-o à lista de certificados confiáveis - nenhuma janela de alerta é exibida para certificados confiáveis.

Não - Marca o certificado como não confiável para a sessão atual - a janela de alerta será exibida na próxima tentativa de usar o certificado.

Excluir - Adiciona o certificado à lista de certificados excluídos - dados transferidos por determinado canal criptografado não serão verificados.

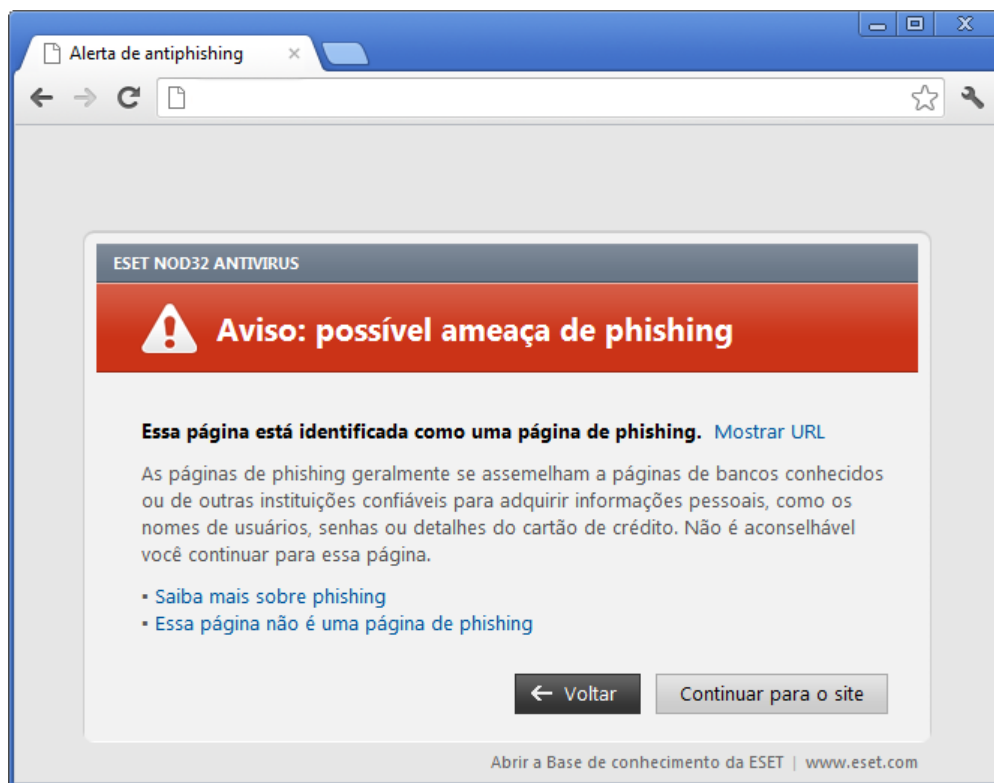
4.2.4 Proteção antiphishing

O termo roubo de identidade define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre essa atividade no glossário. O ESET NOD32 Antivirus oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

Recomendamos que você ative a proteção antiphishing no ESET NOD32 Antivirus. Essa opção pode ser acessada na **Configuração avançada** (F5) acessando **Web e email** > **Proteção antiphishing**.

Consulte também o seguinte Artigo da Base de conhecimento da ESET para obter uma versão atualizada e mais detalhada desta página de ajuda.

Acessando um site de roubo de identidade

Ao acessar um site de roubo de identidade, você verá a caixa de diálogo a seguir no seu navegador da web. Ao clicar em **Continuar no site (não recomendado)**, você poderá acessar o site sem uma mensagem de aviso.

OBSERVAÇÃO: por padrão, sites de roubo de identidade em potencial que tiverem sido permitidos expirarão horas depois. Para permitir um site permanentemente, você pode usar a ferramenta de gerenciamento de endereços de URL. Na **Configuração avançada** (F5), clique em **Web e email** > **Proteção do acesso à web** > **Gerenciamento de endereços de URL** e, no menu suspenso **Gerenciamento de endereços de URL**, selecione **Lista de endereços permitidos** e adicione seu site à essa lista.

Denúncia de site de roubo de identidade

O link Denunciar um site de roubo de identidade permite que você denuncie um site de roubo de identidade/malicioso para análise da ESET.

OBSERVAÇÃO: antes de enviar um site para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o site não foi detectado,
- o site foi detectado incorretamente como uma ameaça. Nesse caso, consulte o link Remover site de roubo de identidade.

Como alternativa, você pode enviar o site por email. Envie seu email para samples@eset.com. Inclua uma linha de assunto clara e o máximo de informações possível sobre o site (por exemplo, o site do qual as obteve, como ouviu falar sobre ele, etc.).

4.3 Atualização do programa

Atualizar o ESET NOD32 Antivirus periodicamente é o melhor método para se garantir o nível máximo de segurança em seu computador. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

Na janela principal do programa, ao clicar em **Atualizar**, você poderá visualizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Além disso, a opção para iniciar manualmente o processo de atualização **Atualizar banco de dados de assinatura de vírus**, está disponível. A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos. Dê atenção especial à sua configuração e operação. Se você não inseriu os detalhes da licença (nome de usuário e senha) durante a instalação, você poderá inserir o nome de usuário e a senha ao atualizar para acessar os servidores de atualização da ESET.

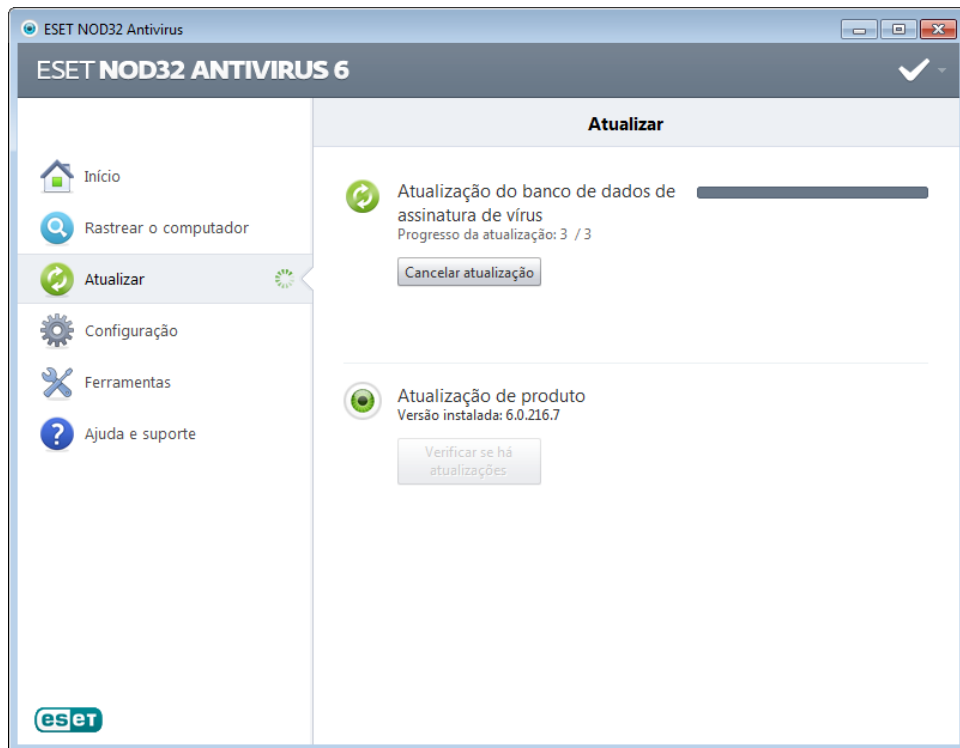
OBSERVAÇÃO: Seu nome de usuário e senha são fornecidos pela ESET após a compra do ESET NOD32 Antivirus.

Última atualização bem-sucedida - A data da última atualização. Se você não vir uma data recente,

Versão do banco de dados de assinatura de vírus – O número do banco de dados de assinatura de vírus, que também é um link ativo para o site da ESET. Clique para exibir uma lista de todas as assinaturas adicionadas na atualização.

Clique em **Verificar** para detectar a versão disponível do ESET NOD32 Antivirus mais recente.

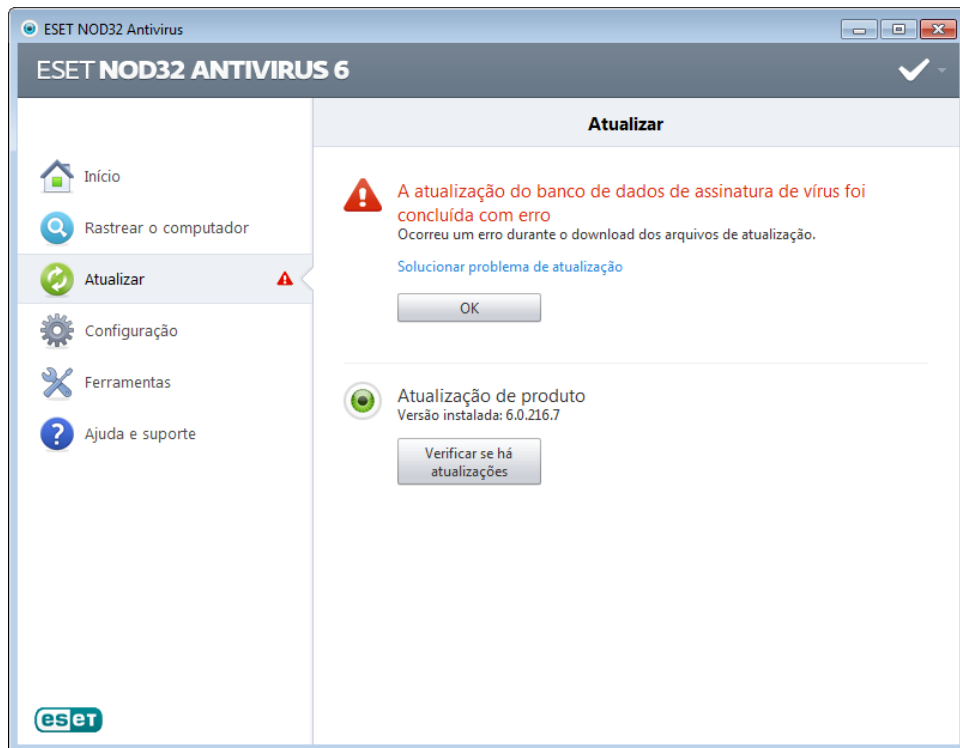
Processo de atualização

Após clicar no botão **Atualizar banco de dados de assinatura de vírus**, o processo de download é iniciado. A barra de progresso do download e o tempo restante do download serão exibidos. Para interromper a atualização, clique em **Cancelar atualização**.

Importante: Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado** aparecerá na janela **Atualizar**. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize o banco de dados de assinatura de vírus assim que for possível. Caso contrário, uma das seguintes mensagens será exibida:

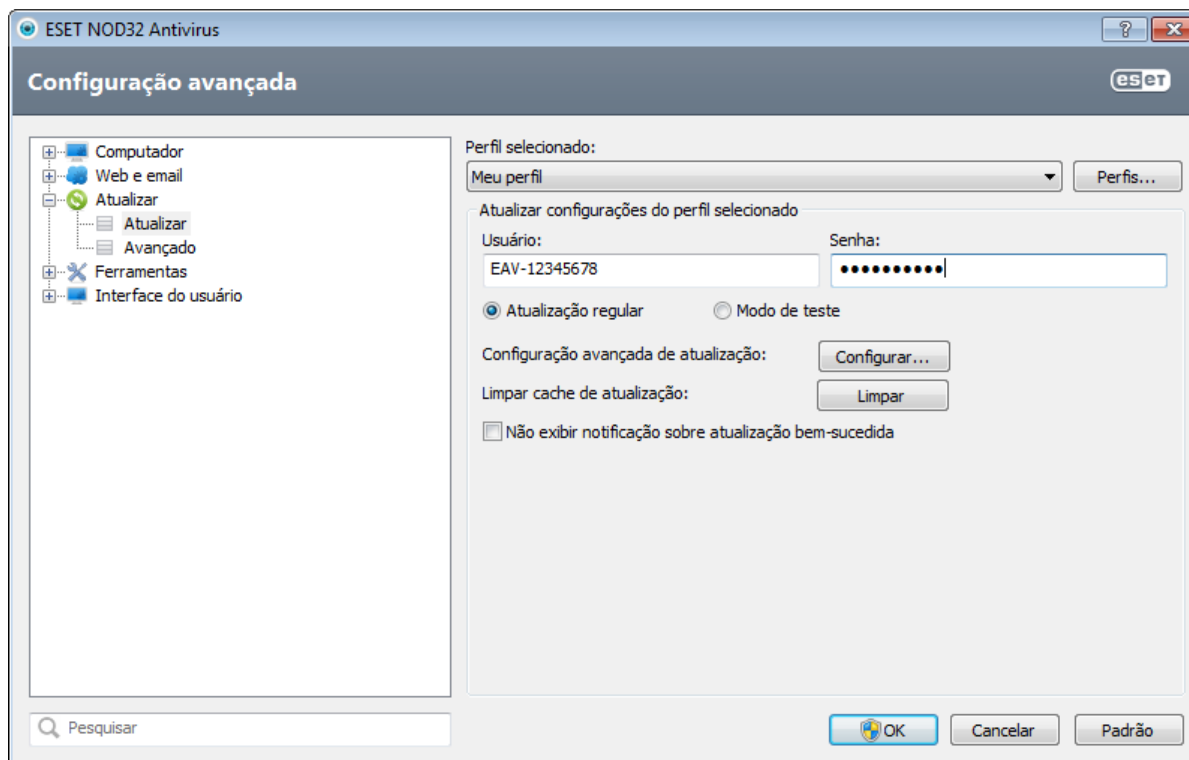
O banco de dados de assinatura de vírus está desatualizado - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o banco de dados de assinatura de vírus. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou as definições incorretas das configurações de conexão.

A notificação anterior está relacionada às duas mensagens a seguir de **Falha na atualização do banco de dados de assinatura de vírus** sobre atualizações malsucedidas:

1. **Usuário e/ou senha inválidos** - O nome de usuário e a senha foram inseridos incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (no menu principal, clique em **Configuração** e escolha a opção **Entrar na configuração avançada...**, ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Atualizar** > **Atualizar** na árvore Configuração avançada para inserir uma nova senha e nome de usuário.

2. **Ocorreu um erro durante o download dos arquivos de atualização** - Uma possível causa do erro pode dever-se a configurações de conexão à Internet incorretas. Recomendamos que você verifique a conectividade da Internet (abrindo qualquer site em seu navegador da Web). Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.

4.3.1 Configuração da atualização

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) clicando em **Atualizar** > **Atualizar**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede.

Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todas as informações de atualização. Se você usar um firewall, certifique-se de que o programa tem permissão para comunicar com a Internet (p. ex., comunicação HTTP).

O perfil de atualização usado atualmente é exibido no menu suspenso **Perfil selecionado**. Clique em **Perfis...** para criar um novo perfil.

A autenticação dos servidores de atualização é baseada no **Usuário** e na **Senha** gerados e enviados ao usuário após a

compra. Por padrão, não é necessário verificação, ou seja, os campos **Usuário** e **Senha** são deixados em branco.

As atualizações em modo de teste (a opção **Modo de teste**) são atualizações que passaram por testes internos e estarão disponíveis de modo geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável, e NÃO DEVE ser usado em servidores de produção e estações de trabalho em que é necessário ter a máxima disponibilidade e estabilidade. A lista dos módulos atuais pode ser encontrada em **Ajuda e suporte** > **Sobre o ESET NOD32 Antivirus**. Se o usuário tiver apenas conhecimentos básicos, é recomendando deixar a opção padrão **Atualização regular** selecionada.

Clique no botão **Configuração...** ao lado de **Configuração avançada de atualização** para exibir uma janela contendo as opções avançadas de atualização.

Se tiver problemas com uma atualização, clique em **Limpar** para excluir arquivos de atualização temporários.

Não exibir notificação sobre atualização bem-sucedida - Desativa a notificação da bandeja do sistema no canto inferior direito da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Lembre-se de que o Modo de jogos desativará todas as notificações.

4.3.1.1 Atualizar perfis

Os perfis de atualização podem ser criados para várias configurações e tarefas de atualização. A criação de perfis de atualização é especialmente útil para usuários móveis, que precisam de um perfil alternativo para propriedades de conexão à Internet que mudam regularmente.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido em **Meu perfil**, por padrão. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil**.

Na janela de configuração de perfis, é possível especificar o servidor de atualização em uma lista de servidores disponíveis ou adicionar um novo servidor. A lista de servidores de atualização existentes está localizada no menu suspenso **Servidor de atualização**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações do perfil selecionado** e, em seguida, clique no botão **Adicionar**.

4.3.1.2 Configuração avançada de atualização

Para visualizar a Configuração avançada de atualização, clique no botão **Configuração...**. As opções de configuração avançada de atualização incluem a configuração do **Modo de atualização**, **Proxy HTTP** e **LAN**.

4.3.1.2.1 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa. O programa permite que você pré-defina seu comportamento quando uma nova atualização de componentes está disponível.

As atualizações de componentes do programa oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador. Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Nunca atualizar componentes do programa** - As atualizações de componentes do programa não serão realizadas. Esta opção é adequada para instalações de servidor, pois os servidores podem geralmente ser reiniciados somente quando estiverem em manutenção.
- **Sempre atualizar componentes do programa** - As atualizações de componentes do programa serão obtidas por download e instaladas automaticamente. Lembre-se de que pode ser necessário reiniciar o computador.
- **Perguntar antes de fazer download dos componentes do programa** - Opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.

Após a atualização de componentes do programa, poderá ser necessário reinicializar o computador para obter uma completa funcionalidade de todos os módulos. A seção **Reiniciar depois da atualização do componente do programa** permite que o usuário selecione uma das três opções a seguir:

- **Nunca reiniciar o computador** - Não será solicitada a reinicialização, mesmo quando for necessária. Observe que isso não é recomendável, pois o computador pode não funcionar adequadamente até a próxima reinicialização.
- **Sugerir opção de reinicialização do computador, se necessário** - Opção padrão. Depois de uma atualização dos componentes do programa, uma janela de diálogo solicitará que você reinicie o computador.
- **Se necessário, reiniciar o computador sem notificar** - Depois de uma atualização dos componentes do programa,

o seu computador será reiniciado (se necessário).

OBSERVAÇÃO: A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

Se a opção **Perguntar antes de fazer download da atualização** estiver marcada, uma notificação será exibida quando uma nova atualização estiver disponível.

Se o tamanho do arquivo de atualização for maior que o valor especificado no campo **Perguntar se um arquivo de atualização for maior que**, o programa exibirá uma notificação.

A opção **Verificar regularmente pela versão mais recente do produto** ativará a tarefa agendada **Verificação regular pela última versão do produto** (consulte Agenda).

4.3.1.2.2 Servidor proxy

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore Configuração avançada (F5) e clique no botão **Configuração...** à direita de **Configuração avançada de atualização**. Clique na guia **Proxy HTTP** e selecione uma das três opções a seguir:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy**

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Ferramentas** > **Servidor proxy** da árvore Configuração avançada.

Selecione a opção **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET NOD32 Antivirus.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

- Deve ser usado um servidor proxy para atualizar o ESET NOD32 Antivirus que seja diferente do servidor proxy especificado nas configurações globais (**Ferramentas** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação, além do **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não foram definidas globalmente, mas o ESET NOD32 Antivirus irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do Internet Explorer durante a instalação do programa; no entanto, se forem alteradas posteriormente (por exemplo, se você alterar o seu provedor de Internet), verifique se as configurações do proxy HTTP estão corretas nesta janela. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

OBSERVAÇÃO: Os dados de autenticação, tais como **Usuário** e **Senha**, são destinados para acessar o servidor proxy. Preencha esses campos somente se um nome de usuário e uma senha forem necessários. Observe que esses campos não são para seu nome de usuário/senha do ESET NOD32 Antivirus e devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

4.3.1.2.3 Conexão à rede

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão.

Para configurar essa conta, clique na guia **Rede**. A seção **Conectar na rede como** fornece as opções **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado**.

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa opção é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário

especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

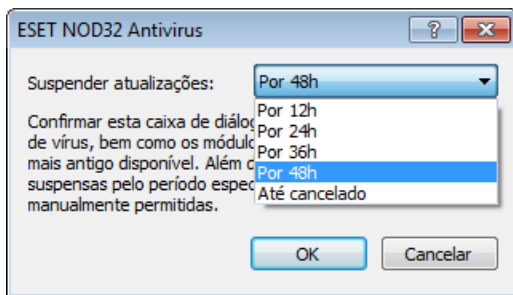
Aviso: Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: *nome_domínio\usuário* (se for um grupo de trabalho, insira o *nome_do_grupo_de_trabalho\nome*) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

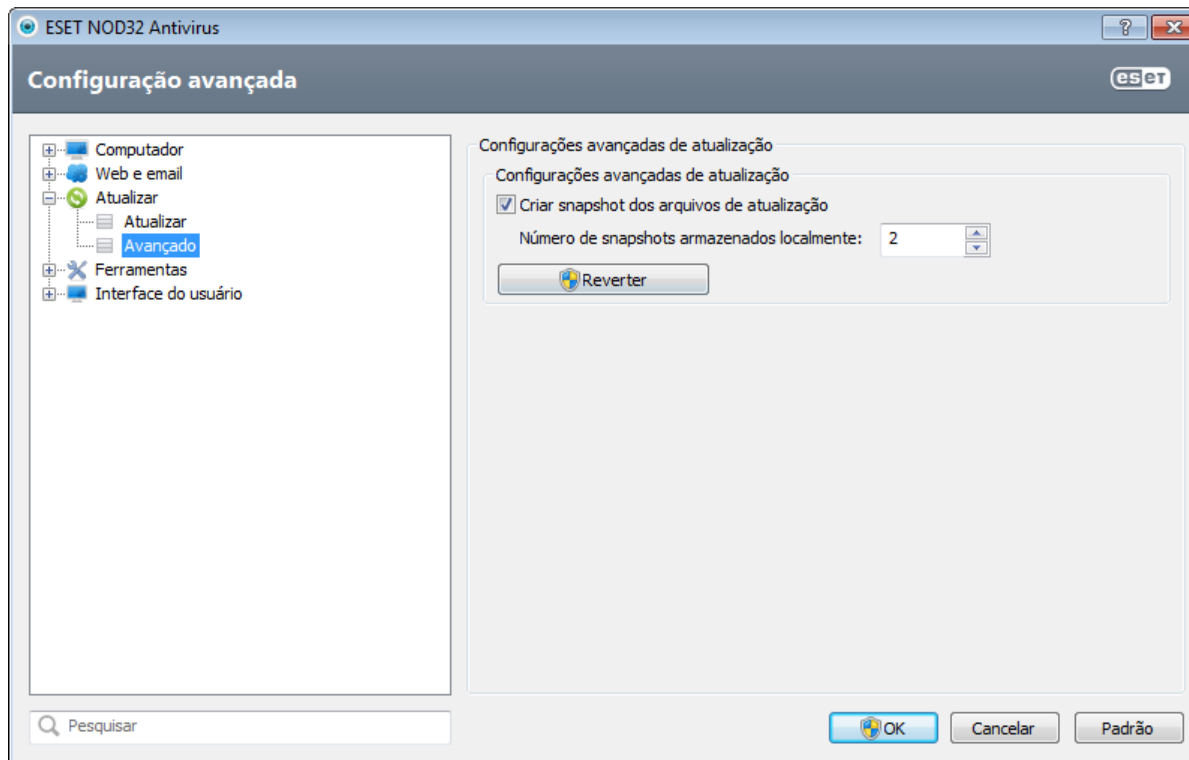
Selecione a opção **Desconectar do servidor depois da atualização** se a conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

4.3.1.3 Rollback de atualização

Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente.

O ESET NOD32 Antivirus registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de *reversão*. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar snapshots dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Avançada**), você terá que selecionar um intervalo de tempo no menu suspenso **Suspender atualizações** que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.

Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

Se uma reversão for realizada, o botão **Reverter** se tornará **Permitir atualizações**. Nenhuma atualização será permitida durante o intervalo de tempo selecionado no menu suspenso **Suspender atualizações**. A versão do banco de dados de assinatura de vírus é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.

Exemplo: Permita que o número 6871 seja a versão mais atual do banco de dados de assinatura de vírus. 6870 e 6868 são armazenados como instantâneos do banco de dados de assinatura de vírus. Observe que 6869 não está disponível porque, por exemplo, o computador foi desligado e uma atualização mais recente foi disponibilizada antes de a 6869 ser baixada. Se você inseriu 2 (dois) no campo **Número de instantâneos armazenados localmente** e clicou em **Reverter**, o banco de dados de assinatura de vírus (incluindo módulos do programa) será restaurado para a versão número 6868. Este processo pode demorar algum tempo. Verifique se a versão do banco de dados de assinatura de vírus foi desatualizada na janela principal do programa do ESET NOD32 Antivirus na seção Atualizar.

4.3.2 Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET NOD32 Antivirus:

- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**

Toda tarefa de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda.

4.4 Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

Esse menu inclui as seguintes ferramentas:

- Arquivos de log
- Estatísticas da proteção
- Monitorar atividade
- Processos em execução
- Agenda
- Quarentena
- ESET SysInspector

Enviar arquivo para análise - Permite enviar um arquivo suspeito aos Laboratórios de vírus da ESET para análise. A janela de diálogo exibida depois de clicar nessa opção é descrita na seção Envio de arquivos para análise.

ESET SysRescue - Inicia o assistente de criação do ESET SysRescue.

ESET Social Media Scanner - Link para um aplicativo de mídia social (p. ex., Facebook) com objetivo de proteger usuários de mídia social contra ameaças. Este apliactivo é independente de outros produtos de segurança da ESET e é totalmente gratuito.

4.4.1 Arquivos de log

Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log é uma parte essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do log. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET NOD32 Antivirus, bem como arquivar logs.

Os arquivos de log podem ser acessados na janela principal do programa, clicando em **Ferramentas** > **Arquivos de log**. Selecione o tipo de log desejado no menu suspenso **Log** Os seguintes logs estão disponíveis:

- **Ameaças detectadas** - O log de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelos módulos do ESET NOD32 Antivirus. As informações incluem a hora da detecção, nome da ameaça, local, ação realizada e o nome do usuário conectado no momento em que a ameaça foi detectada. Clique duas vezes em qualquer entrada de log para exibir seus detalhes em uma janela separada.

- **Eventos** - Todas as ações importantes executadas pelo ESET NOD32 Antivirus são registradas no log de eventos. O log de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para a solução de problemas de administradores do sistema e de usuários. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.

- **Rastrear o computador** - Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo rastreamento.

- **HIPS** - Contém registros de regras específicas do HIPS que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.

- **Sites filtrados** - Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela Proteção de acesso à web. Nesses logs, você poderá ver o horário, endereço URL, usuário e aplicativo que criaram uma conexão para o site específico.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência (atalho do teclado: Ctrl + C), selecionando a entrada e clicando em **Copiar**. Para selecionar várias entradas, as teclas CTRL e SHIFT podem ser usadas.

Você pode exibir o menu de contexto clicando com o botão direito em uma determinada entrada. As seguintes opções também estão disponíveis no menu de contexto.

- **Filtrar registros do mesmo tipo** - Depois de ativar esse filtro, você só verá registros do mesmo tipo (diagnósticos, avisos...).
- **Filtrar.../Localizar...** - Depois de clicar nessa opção, uma janela chamada **Filtragem de logs** será aberta e você poderá definir os critérios de filtragem.
- **Desativar filtro** - Apaga todas as configurações do filtro (conforme descrição acima).
- **Copiar tudo** - Copia informações sobre todos os registros na janela.
- **Excluir/Excluir tudo** - Exclui o(s) registro(s) selecionado(s) ou todos os exibidos - essa ação requer privilégios de administrador.
- **Exportar** - Exporta informações sobre o(s) registro(s) em formato XML.
- **Percorrer log** - Deixe esta opção ativada para percorrer automaticamente logs antigos e monitorar logs ativos na janela **Arquivos de log**.

4.4.1.1 Manutenção de logs

A configuração de logs do ESET NOD32 Antivirus pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Arquivos de log**. A seção de logs é utilizada para definir como os logs serão gerenciados. O programa exclui automaticamente os logs mais antigos a fim de economizar espaço no disco rígido. Você pode especificar as seguintes opções para logs:

As entradas de logs anteriores ao número de dias especificado no campo **Excluir registros anteriores a X dias** são automaticamente excluídas.

Otimizar automaticamente arquivos de log - Se selecionada, os arquivos de log serão automaticamente desfragmentados se a porcentagem for superior ao valor especificado no campo **Se o número de registros não utilizados excede (%)**.

Clique em **Otimizar agora** para iniciar a desfragmentação dos arquivos de log. Todas as entradas de logs vazias são removidas durante esse processo, o que melhora o desempenho e a velocidade no processamento de logs. Essa

melhoria pode ser observada especialmente se os logs tiverem um grande número de entradas.

Detalhamento mínimo de registro em log - Especifica o nível de detalhamento mínimo de eventos a serem registrados em log.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como *"Erro ao fazer download de arquivo"* e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc...).

Clique no botão **Filtro padrão...** para abrir a janela **Filtragem de logs**. Verifique os tipos de registro a serem exibidos em logs e clique em **OK**.

4.4.2 Agenda

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas.

A Agenda pode ser acessada na janela principal do programa do ESET NOD32 Antivirus em **Ferramentas** > **Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

O Agendador serve para agendar as seguintes tarefas: atualização do banco de dados das assinaturas de vírus, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do log. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar...** ou **Excluir** na parte inferior). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa e excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção de logs**
- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**
- **Verificação regular pela última versão do produto** (consulte Modo de atualização)
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Verificação automática de arquivos durante inicialização do sistema** (após atualização bem-sucedida do banco de dados de assinatura de vírus)

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

Adicionar uma nova tarefa

1. Clique em **Adicionar...** na parte inferior da janela.

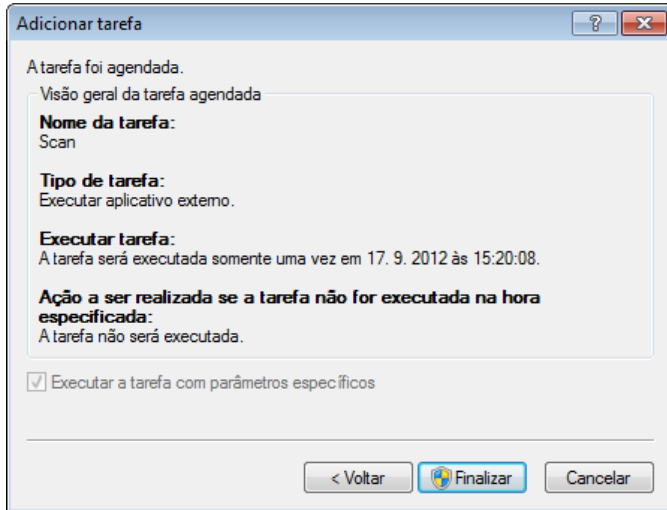
2. Selecione a tarefa desejada no menu suspenso.

3. Insira o nome da tarefa e selecione uma das seguintes opções de tempo:

   - **Uma vez** - A tarefa será realizada somente uma vez, na data e hora predefinidas.
   - **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado (em horas).
   - **Diariamente** - A tarefa será realizada diariamente na hora especificada.
   - **Semanalmente** - A tarefa será realizada uma ou mais vezes por semana, no(s) dia(s) e hora selecionados.
   - **Evento disparado** - A tarefa será realizada após um evento especificado.

4. Dependendo da opção de tempo escolhida na etapa anterior, uma destas janelas de diálogo será exibida:

   - **Uma vez** - A tarefa será realizada na data e hora predefinidas.
   - **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
   - **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
   - **Semanalmente** - A tarefa será realizada na data e hora selecionadas.

5. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:
    - Aguardar até a próxima hora agendada
    - Executar a tarefa tão logo quanto possível
    - Executar a tarefa imediatamente se o período de tempo desde a última execução da tarefa for maior que -- horas
6. Na última etapa, você pode revisar a tarefa agendada. Clique em **Concluir** para aplicar a tarefa.

4.4.3 Estatísticas da proteção

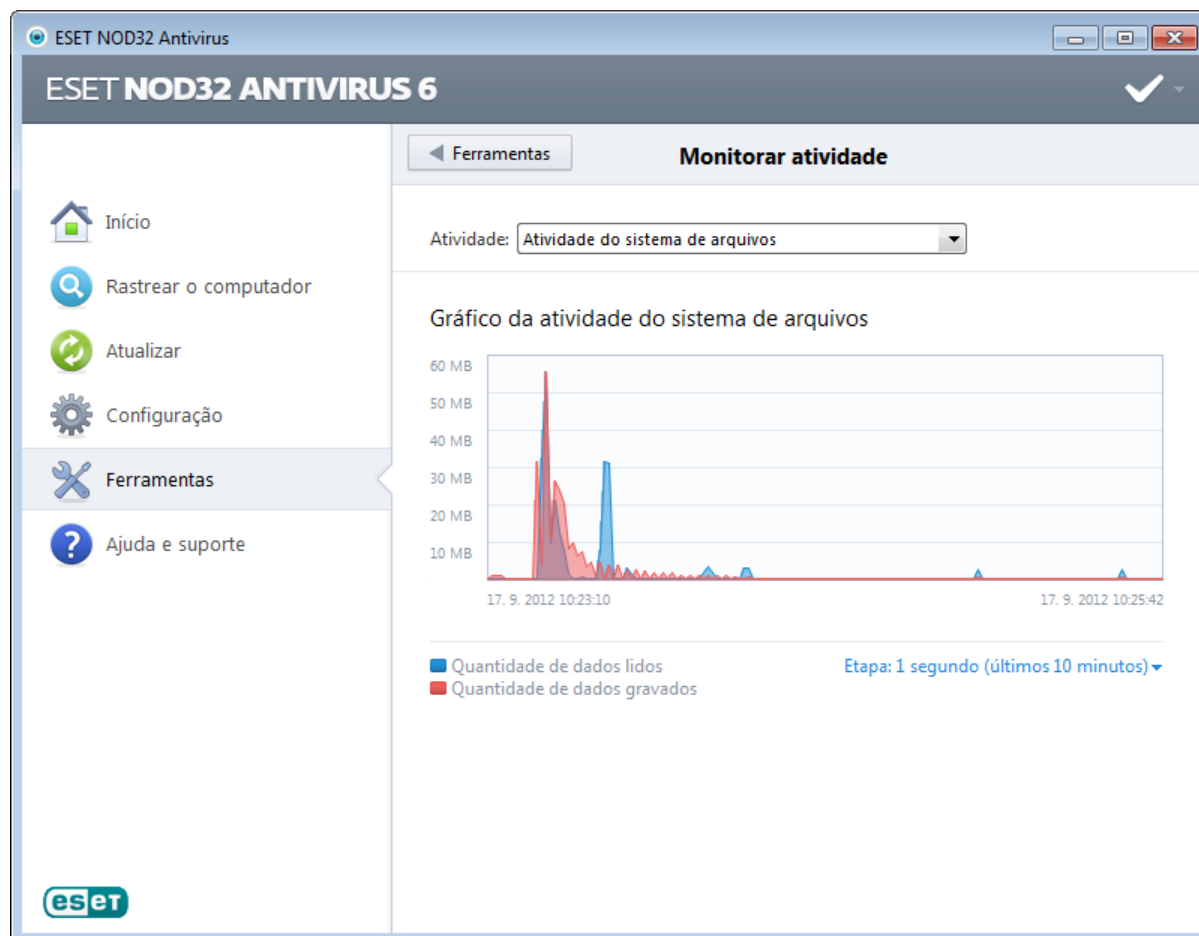
Para exibir um gráfico de dados estatísticos relacionados aos módulos de proteção do ESET NOD32 Antivirus, clique em **Ferramentas** > **Estatísticas da proteção**. Selecione o módulo de proteção desejado no menu suspenso **Estatísticas** para visualizar o gráfico e a legenda correspondentes. Se você passar o mouse sobre um item na legenda, somente os dados desse item serão exibidos no gráfico.

Os gráficos estatísticos a seguir estão disponíveis:

- **Proteção antifírus e antispyware** - Exibe o número de objetos infectados e limpos.
- **Proteção do sistema de arquivos** - Exibe apenas os objetos que foram lidos ou gravados no sistema de arquivos.
- **Proteção do cliente de email** - Exibe apenas os objetos que foram enviados ou recebidos pelos clientes de email.
- **Proteção antiphishing e de acesso à Web** - Exibe apenas os objetos obtidos por download pelos navegadores da web.

Abaixo dos gráficos de estatísticas, você pode ver o número total de objetos rastreados, o último objeto rastreado e o registro de estatísticas. Clique em **Redefinir** para apagar todas as informações estatísticas.

4.4.4 Monitorar atividade

Para visualizar a **Atividade do sistema de arquivos** atual em forma gráfica, clique em **Ferramentas** > **Monitorar atividade**. Na parte inferior do gráfico, há uma linha do tempo que grava a atividade do sistema de arquivos em tempo real com base na duração do tempo selecionado. Para alterar a duração do tempo, clique na opção **Etapa: 1...**, localizada no canto inferior direito da janela.

As opções disponíveis são:

- **Etapa: 1 segundo (últimos 10 minutos)** - O gráfico é atualizado a cada segundo e a linha de tempo cobre os últimos 10 minutos
- **Etapa: 1 minuto (últimas 24 horas)** - O gráfico é atualizado a cada minuto e a linha de tempo cobre as últimas 24 horas
- **Etapa: 1 hora (último mês)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês
- **Etapa: 1 hora (mês selecionado)** - O gráfico é atualizado a cada hora e a linha de tempo cobre os últimos X meses selecionados

O eixo vertical do **Gráfico da atividade do sistema de arquivos** representa os dados lidos (azul) e os dados gravados (vermelho). Ambos os valores são fornecidos em KB (kilobytes)/MB/GB. Se você passar o mouse sobre os dados lidos ou sobre os dados gravados na legenda embaixo do gráfico, apenas os dados para esse tipo de atividade serão exibidos no gráfico.

4.4.5 ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos instalados, as conexões de rede ou entradas de registo importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware.

A janela do SysInspector exibe as seguintes informações sobre os logs criados:

- **Hora** - A hora de criação do log.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o log.
- **Status** - O status de criação do log.

As seguintes ações estão disponíveis:

- **Comparar** - Compara dois logs existentes.
- **Criar...** - Cria um novo log. Aguarde até que o log do ESET SysInspector seja concluído (**Status** exibido como Criado).
- **Excluir** - Remove os logs selecionados da lista.

Após clicar com o botão direito em um ou mais logs selecionados, as seguintes opções estarão disponíveis no menu de contexto:

- **Mostrar** - Abre o log selecionado no ESET SysInspector (igual a clicar duas vezes em um log).
- **Excluir tudo** - Exclui todos os logs.
- **Exportar...** - Exporta o log para um arquivo *.xml* ou *.xml* compactado.

4.4.6 ESET Live Grid

O ESET Live Grid (a próxima geração do ThreatSense.Net) é um sistema de avisos avançado contra ameaças emergentes com base na reputação. Usando a transmissão contínua em tempo real de informações relacionadas a ameaças da nuvem, o laboratório de vírus da ESET mantém as defesas atualizadas para oferecer um nível de proteção constante. O usuário pode verificar a reputação dos arquivos e dos processos em execução diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET Live Grid. Há duas opções:

1. Você decide se deseja ou não ativar o ESET Live Grid. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.
2. É possível configurar o ESET Live Grid para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ESET Live Grid coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET NOD32 Antivirus é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como *.doc* ou *.xls*, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

O menu de configuração do ESET Live Grid fornece várias opções para ativar/desativar o ESET Live Grid, que serve para enviar arquivos suspeitos e informações estatísticas anônimas para os laboratórios da ESET. Ele pode ser acessado a partir da árvore Configuração avançada clicando em **Ferramentas** > **ESET Live Grid**.

Participar do ESET Live Grid (recomendado) - Ativa/desativa o ESET Live Grid, que serve para enviar arquivos suspeitos e informações estatísticas anônimas para os laboratórios da ESET.

Não enviar estatísticas – Selecione essa opção se você não quiser enviar informações anônimas a partir do ESET Live Grid sobre seu computador. Essas informações estão relacionadas às ameaças detectadas recentemente que podem incluir o nome da infiltração, informação sobre a data e hora em que ela foi detectada, a versão do ESET NOD32 Antivirus, informações sobre o sistema operacional do computador e as configurações de Local. As estatísticas são geralmente entregues ao servidor da ESET uma ou duas vezes ao dia.

Não enviar arquivos – Arquivos suspeitos, que se pareçam com infiltrações em seus conteúdos ou comportamento, não são enviados à ESET para análise por meio da tecnologia ESET Live Grid.

Configuração avançada... - Abre uma janela com configurações adicionais do ESET Live Grid.

Se já tiver usado o ESET Live Grid antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET na próxima ocasião. Posteriormente, não serão criados pacotes adicionais.

4.4.6.1 Arquivos suspeitos

A guia **Arquivos** da configuração avançada do ESET Live Grid permite configurar como as ameaças serão enviadas ao Laboratório de vírus da ESET para análise.

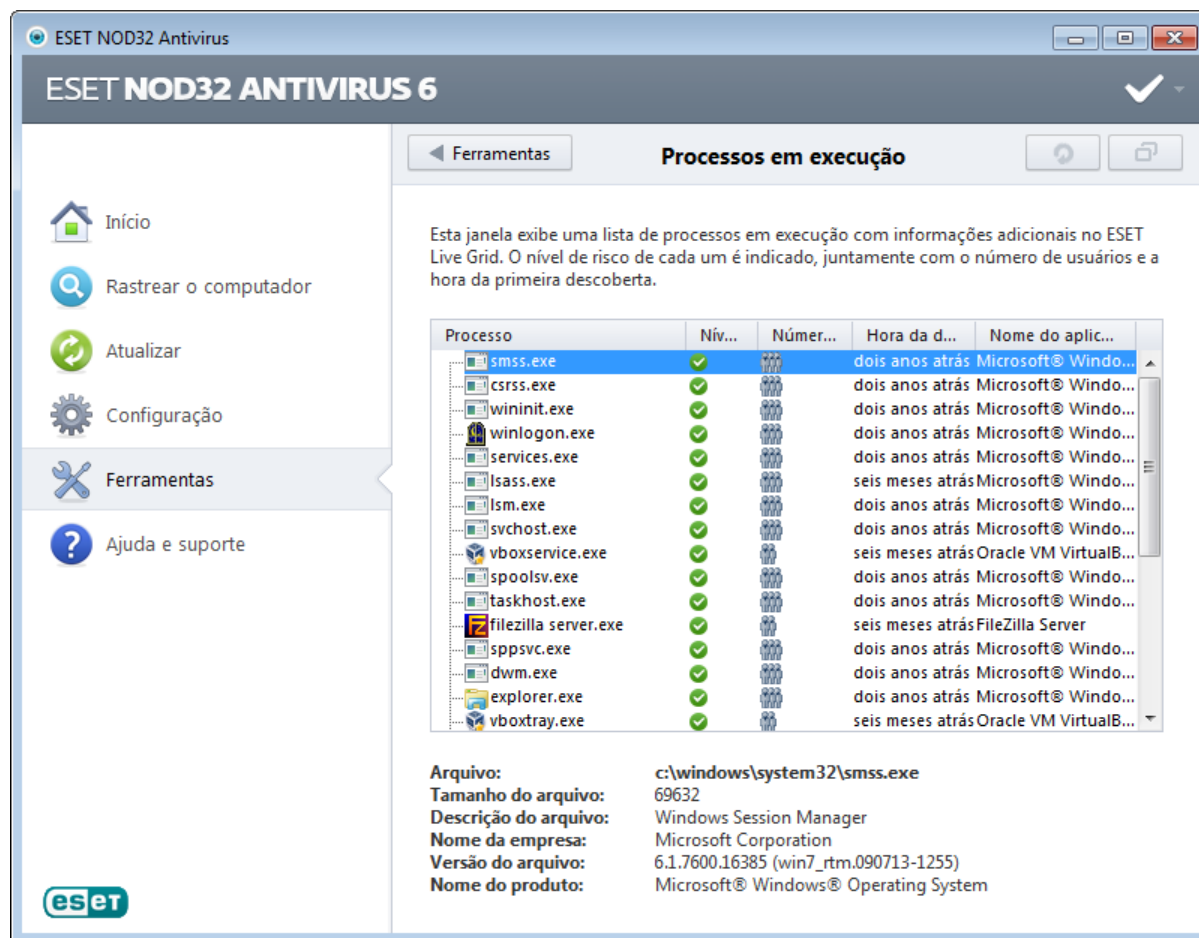
Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

Filtro de exclusões - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Selecione a opção **Ativar registro em log** para criar um log de eventos para registrar os envios de arquivos e informações estatísticas. Ela permite o registro no Log de eventos quando arquivos ou estatísticas são enviados.

4.4.7 Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET NOD32 Antivirus oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia ESET Live Grid.

Processo - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção Gerenciador de tarefas ou pressionando Ctrl+Shift+Esc no teclado.

Nível de risco - Na maioria dos casos, o ESET NOD32 Antivirus e a tecnologia ESET Live Grid atribui níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 – Aceitável (verde) a 9 – Perigoso (vermelho).

OBSERVAÇÃO: Aplicativos conhecidos marcados como Aceitável (verde) são limpos definitivamente (lista de permissões) e serão excluídos do rastreamento, pois isso melhorará a velocidade do rastreamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

Número de usuários - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ESET Live Grid.

Hora da descoberta - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ESET Live Grid.

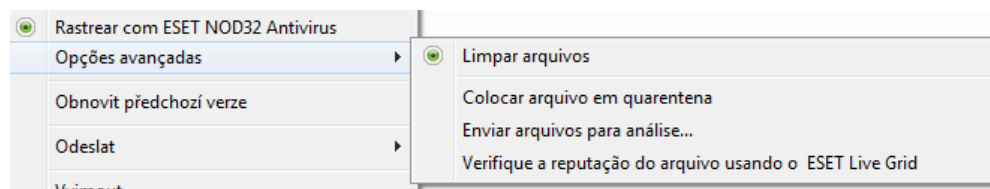
OBSERVAÇÃO: Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se não tiver certeza sobre o arquivo, você poderá enviar o arquivo para análise ao Laboratório de Vírus da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Nome do aplicativo - O nome de um programa ou processo.

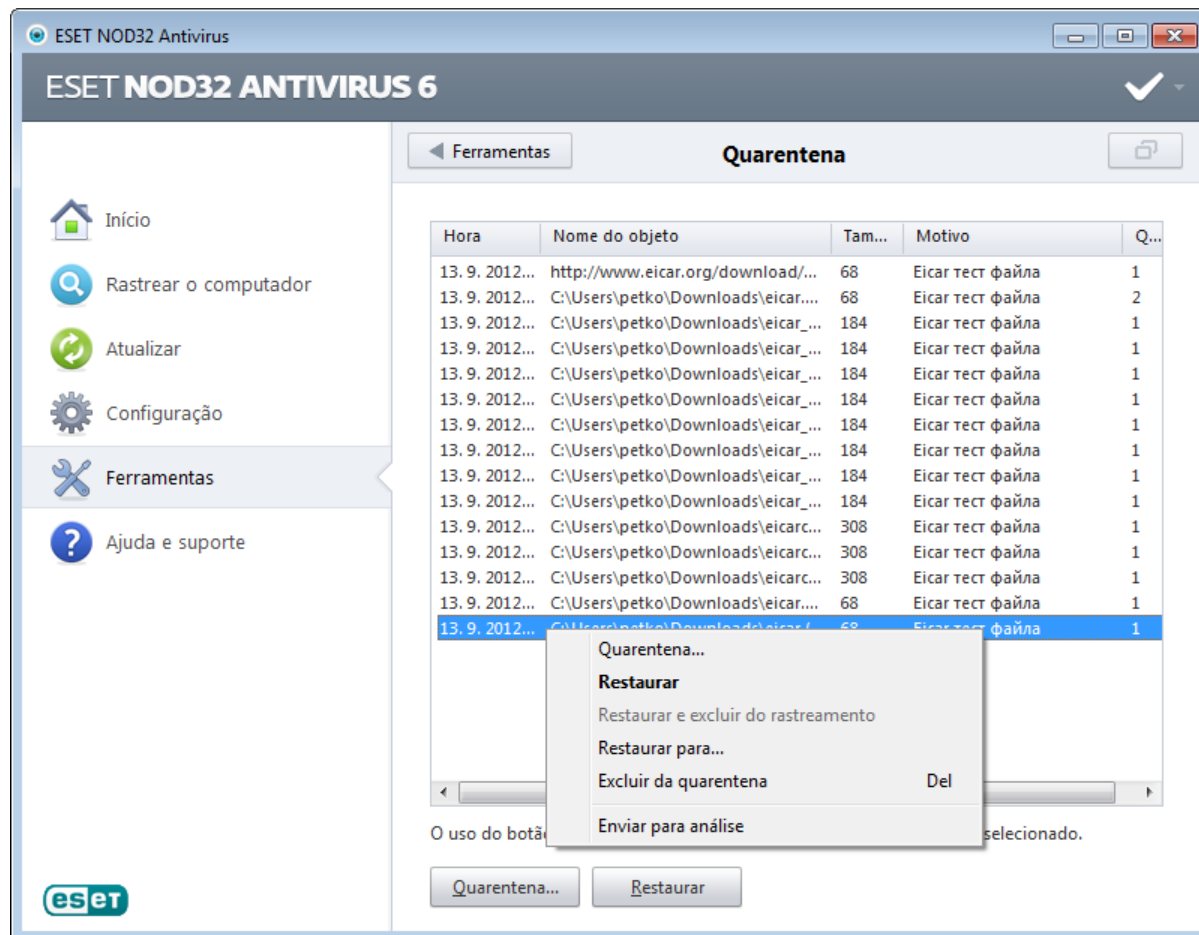
Abrir em uma nova janela - As informações dos processos em execução serão abertas em uma nova janela.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

- **Arquivo** - Local de um aplicativo no computador.
- **Tamanho do arquivo** - Tamanho do arquivo em B (bytes).
- **Descrição do arquivo** - Características do arquivo com base na descrição do sistema operacional.
- **Nome da empresa** - Nome de processo do aplicativo ou do fornecedor.
- **Versão do arquivo** - Informações do editor do aplicativo.
- **Nome do produto** - Nome do aplicativo e/ou nome comercial.

OBSERVAÇÃO: a reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e selecione **Opções avançadas** > **Verificar reputação do arquivo usando o ESET Live Grid**.

4.4.8 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET NOD32 Antivirus.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de vírus da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

Colocação de arquivos em quarentena

O ESET NOD32 Antivirus coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena...**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena...**

Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Utilize o recurso **Restaurar** para essa finalidade, que está disponível no menu de contexto clicando com o botão direito do mouse no arquivo desejado, na janela Quarentena. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, a opção **Restaurar e excluir do rastreamento** será ativada. Leia mais sobre esse tipo de aplicativo no glossário. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO: se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao Cliente da ESET.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.4.9 Configuração do servidor proxy

Em grandes redes, a conexão do seu computador com a Internet pode ser mediada por um servidor proxy. Se esse for o caso, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não poderá se atualizar automaticamente. No ESET NOD32 Antivirus, a configuração do servidor proxy está disponível em duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET NOD32 Antivirus. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

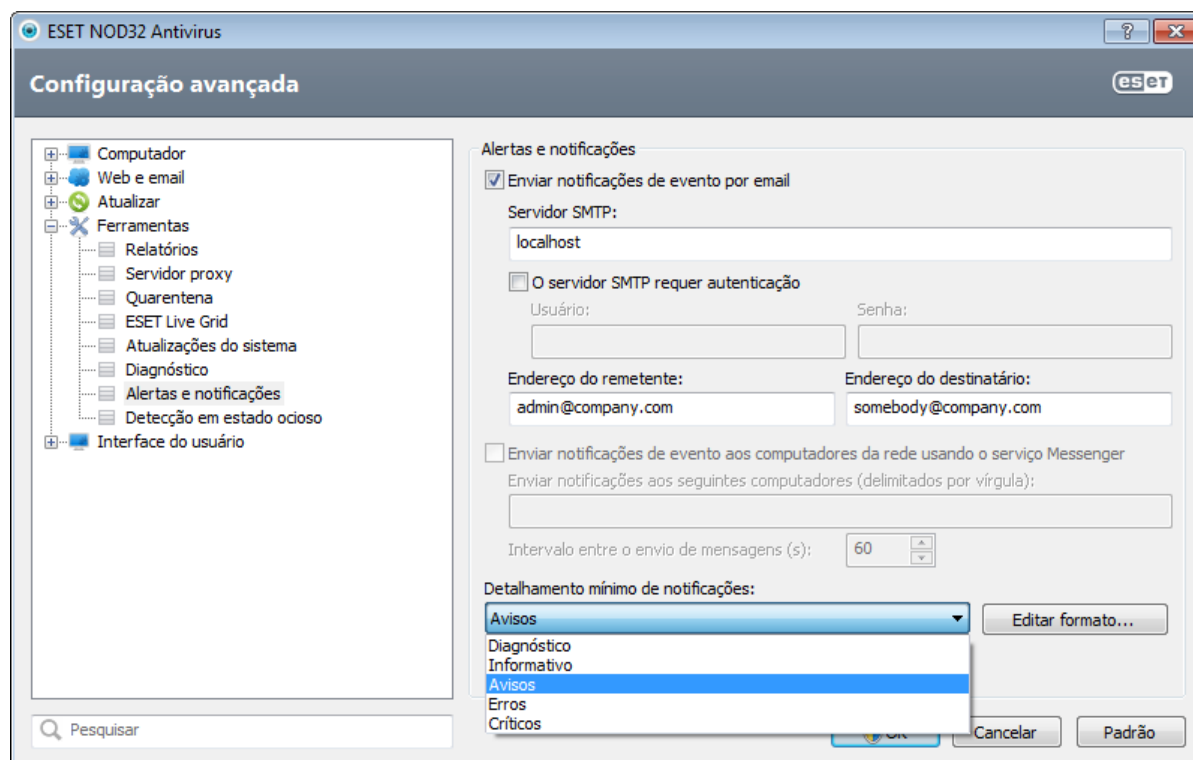
Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

OBSERVAÇÃO: Esse recurso não recupera dados de autenticação (nome de usuário e senha); eles devem ser fornecidos por você.

As configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (ramificação **Atualizar** da árvore **Configuração avançada**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações de assinatura de vírus de diferentes locais. Para obter mais informações sobre essa configuração, consulte a seção Configuração avançada de atualização.

4.4.10 Alertas e notificações

O ESET NOD32 Antivirus suportará o envio de emails se um evento com o nível de detalhamento selecionado ocorrer. Clique na caixa de seleção **Enviar notificações de evento por email** para ativar este recurso e ativar as notificações por e-mail.

Servidor SMTP - O servidor SMTP usado para o envio de notificações.

Observação: Os servidores SMTP com criptografia SSL/TLS não são suportados pelo ESET NOD32 Antivirus.

O servidor SMTP requer autenticação - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos, concedendo acesso ao servidor SMTP.

Endereço do remetente - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.

Endereço do destinatário - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação.

Enviar notificações de evento aos computadores da rede usando o serviço Messenger - Marque esta caixa de seleção para enviar mensagens para computadores na rede local por meio do serviço de mensagem do Windows®.

Enviar notificações aos seguintes computadores (delimitados por vírgula) - Insira os nomes dos computadores que receberão notificações por meio do serviço de mensagens do Windows®.

Intervalo entre o envio de mensagens (s) - Para alterar a duração do intervalo entre notificações enviadas por meio da rede local, digite o intervalo de tempo desejado em segundos.

Detalhamento mínimo de notificações - Especifica o nível de detalhamento mínimo de notificações a serem enviadas.

Editar formato... - As comunicações entre o programa e um usuário remoto ou administrador do sistema são feitas por meio de emails ou mensagens de rede local (usando o serviço de mensagens do Windows®). O formato padrão das mensagens de alerta e notificações será o ideal para a maioria das situações. Em algumas circunstâncias, você pode precisar alterar o formato da mensagem - clique em Editar formato....

4.4.10.1 Formato de mensagem

Aqui é possível configurar o formato das mensagens de eventos que são exibidas em computadores remotos.

As mensagens de alerta e notificação de ameaças têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

As palavras-chave (cadeias de caractere separadas por sinais %) são substituídas na mensagem pelas informações reais conforme especificadas. As palavras-chave disponíveis são:

- **%TimeStamp%** - Data e hora do evento.
- **%Scanner%** - Módulo relacionado.
- **%ComputerName%** - Nome do computador no qual o alerta ocorreu.
- **%ProgramName%** - Programa que gerou o alerta.
- **%InfectedObject%** - Nome do arquivo e mensagem infectados etc.
- **%VirusName%** - Identificação da infecção.
- **%ErrorDescription%** - Descrição de um evento não vírus.

As palavras-chave **%InfectedObject%** e **%VirusName%** são usadas somente em mensagens de alerta de ameaça, enquanto **%ErrorDescription%** é usada somente em mensagens de evento.

Utilizar caracteres do alfabeto local - Converte uma mensagem de email para a codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").

Utilizar codificações de caracteres locais - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

4.4.11 Envio de arquivos para análise

A caixa de diálogo de envio de arquivos permite enviar um arquivo para a ESET para fins de análise e pode ser acessada em **Ferramentas** > **Enviar arquivo para análise**. Se você detectar um arquivo com comportamento suspeito no seu computador, poderá enviá-lo para o Laboratório de vírus da ESET para análise. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/ZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, o site do qual fez o download).

OBSERVAÇÃO: Antes de enviar um arquivo para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:
- o arquivo não foi detectado,
- o arquivo foi detectado incorretamente como uma ameaça.

Você não receberá uma resposta, a não ser que mais informações sejam necessárias para a análise.

Selecione a descrição no menu suspenso **Motivo para envio do arquivo** mais adequada à sua mensagem:
- **Arquivo suspeito**,
- **Falso positivo** (arquivo que é detectado como uma infecção, mas que não está infectado),
- e **Outros**.

Arquivo - O caminho do arquivo que você pretende enviar.

Email de contato - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias, pois a cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios.

4.4.12 Atualizações do sistema

O recurso de atualização do Windows é um componente importante de proteção de usuários contra software malicioso. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET NOD32 Antivirus o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas para download.
- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. Assim, as informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

4.5 Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa.

Usando a ferramenta Gráficos, é possível ajustar a aparência visual do programa e os efeitos usados.

Ao configurar Alertas e notificações, você pode alterar o comportamento de alertas de ameaças detectadas e notificações do sistema. Esses recursos podem ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área Janelas de notificação ocultas. Aqui é possível verificar o status dessas notificações, mostrar mais detalhes ou removê-las dessa janela.

Para obter a máxima segurança do seu software, você pode evitar quaisquer alterações não autorizadas protegendo as configurações com uma senha com a ajuda da ferramenta Configuração de acesso.

O Menu de contexto é exibido após um clique com o botão direito do mouse em um objeto. Utilize essa ferramenta para integrar os elementos de controle do ESET NOD32 Antivirus no menu de contexto.

O Modo de jogos é útil para usuários que querem trabalhar com um aplicativo sem interrupções. No modo de jogos, janelas pop-up, tarefas agendadas e quaisquer outros componentes que poderiam diminuir o desempenho são suprimidos.

4.5.1 Gráficos

As opções de configuração da interface do usuário no ESET NOD32 Antivirus permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na árvore Configuração avançada expandindo-se **Interface do usuário** e clicando-se em **Gráficos**.

Na seção **Elementos da interface do usuário**, a opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do seu computador ou provocarem outros problemas. A interface gráfica também pode precisar ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais usados para leitura do texto exibido na tela.

Se desejar desativar a tela inicial do ESET NOD32 Antivirus, desmarque a opção **Mostrar tela inicial na inicialização**.

Habilite a opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento realçado será ativado após um clique no mouse.

Para ativar o uso de ícones animados para exibir o andamento de várias operações, selecione a opção **Usar ícones animados para indicação de progresso**.

Se desejar que o programa emita um aviso sonoro se um evento importante ocorrer, selecione a opção **Usar sinal sonoro**. Observe que esse som será reproduzido somente quando um rastreamento de computador estiver em execução ou tiver sido concluído.

4.5.2 Alertas e notificações

A seção **Alertas e notificações** em **Interface do usuário** permite que você configure como os alertas de ameaças e as notificações do sistema (por exemplo, mensagens de atualização bem-sucedida) são tratados no ESET NOD32 Antivirus. Você também pode definir a hora e o nível de transparência das notificações da bandeja do sistema (aplica-se somente aos sistemas compatíveis com notificações na bandeja do sistema).

Desmarcar a caixa de seleção ao lado de **Exibir alertas** cancelará todas as janelas de alerta e é adequado apenas em determinadas situações. Para a maioria dos usuários, recomendamos que essa opção seja mantida ativada (padrão).

As notificações na área de trabalho são apenas informativas e não requerem nem proporcionam interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar as notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas, como o tempo de exibição e a transparência da janela de notificação, podem ser modificadas clicando no botão **Configurar notificações**. Para visualizar o comportamento das notificações, clique no botão **Visualizar**. Selecione **Não exibir notificações ao executar aplicativos em modo tela cheia** para suprimir notificações ao executar aplicativos em modo tela cheia.

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente depois de (s)**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

Clique em **Configuração avançada** para acessar opções de configuração adicionais de **Alertas e notificações**.

4.5.2.1 Configuração avançada

No menu suspenso **Detalhamento mínimo de eventos para exibir**, é possível selecionar o nível de gravidade inicial dos alertas e das notificações a serem exibidos.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como *"Erro ao fazer download de arquivo"* e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc...).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é

especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

4.5.3 Janelas de notificação ocultas

Se a opção **Não exibir esta mensagem novamente** foi selecionada para qualquer janela de notificação (alerta) que foi exibida anteriormente, ela aparecerá na lista de janelas de notificações ocultas. As ações que agora são executadas automaticamente serão exibidas na coluna **Confirmar**.

Mostrar - Mostra uma visualização das janelas de notificação que não são exibidas no momento e para as quais uma ação automática está configurada.

Remover - Remove itens da lista de **Caixas de mensagens ocultas**. Todas as janelas de notificação removidas da lista serão exibidas novamente.

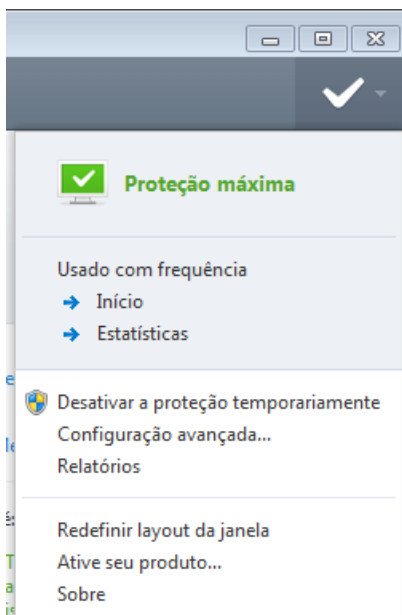
4.5.4 Configuração do acesso

As configurações do ESET NOD32 Antivirus são uma parte essencial de sua política de segurança. Modificações não autorizadas podem colocar em risco a estabilidade e a proteção do seu sistema. Para proteger com senha os parâmetros de configuração, acesse o menu principal e clique em **Configurar** > **Entrar na configuração avançada...** > **Interface do usuário** > **Configuração de acesso**, selecione a opção **Configurações protegidas por senha** e clique no botão **Configurar senha** Observe que a senha diferencia maiúsculas de minúsculas.

Exigir direitos totais de administrador para contas de administrador limitadas - Selecione essa opção para solicitar que o usuário atual (se ele não tiver direitos de administrador) digite o nome de usuário e a senha de administrador quando modificar determinados parâmetros do sistema (semelhante ao UAC no Windows Vista e Windows 7). Essas alterações incluem a desativação dos módulos de proteção. Em sistemas Windows XP nos quais o UAC não estiver em execução, os usuários terão a opção **Exigir direitos de administrador (sistema sem suporte UAC)** disponível.

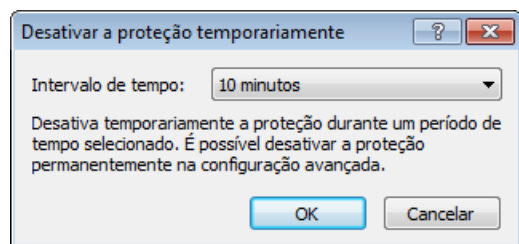
Mostrar caixa de diálogo de tempo limite da proteção - Marcar essa opção fará com que uma janela da caixa de diálogo, denotando a duração do tempo restante com a proteção desativada, seja exibida a qualquer momento em que você desativar temporariamente a proteção do menu do programa ou na seção **ESET NOD32 Antivirus** > **Configuração**.

4.5.5 Menu do programa

No menu principal do programa estão disponíveis alguns dos recursos e opções de configuração mais importantes.

Usado com frequência - Exibe as extensões mais utilizadas do ESET NOD32 Antivirus. Você pode acessar rapidamente esses objetos a partir do menu do programa.

Desativar a proteção temporariamente - Exibe a caixa de diálogo de confirmação que desativa a Proteção antivírus e antispyware, que protege contra ataques maliciosos ao sistema controlando arquivos e a comunicação via web e por emails. Selecione **Não perguntar novamente** para evitar que essa mensagem seja exibida no futuro.

O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção antivírus e antispyware será

desativada.

Configuração avançada... - Selecione essa opção para acessar a árvore **Configuração avançada**. Existem também outras formas de abri-lo, como, por exemplo, pressionando a tecla F5 ou navegando até **Configuração** > **Entrar na configuração avançada...**.

Arquivos de log - Os arquivos de log contêm informações sobre eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas.

Redefinir layout da janela - Redefine a janela do ESET NOD32 Antivirus para seu tamanho e posição padrão na tela.

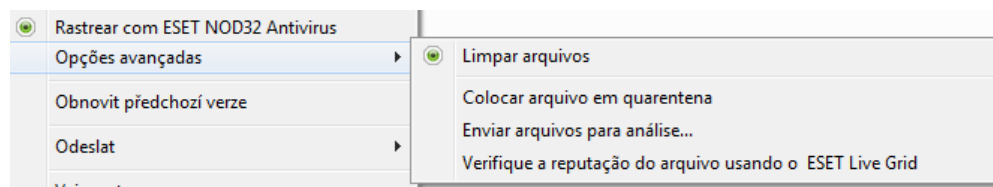
Ativação do produto... - Selecione esta opção se ainda não tiver ativado seu produto de segurança da ESET, ou reinsira as credenciais de ativação do produto depois de renovar sua licença.

Sobre - As informações do sistema fornecem detalhes sobre a versão instalada do ESET NOD32 Antivirus e os componentes do programa instalados. Aqui, você também pode encontrar a data de expiração de licença e informações sobre o sistema operacional e os recursos do sistema.

4.5.6 Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse em um objeto. O menu lista todas as opções disponíveis para executar no objeto.

É possível integrar os elementos de controle do ESET NOD32 Antivirus no menu de contexto. Opções de configuração mais detalhadas para essa funcionalidade estão disponíveis na árvore Configuração avançada em **Interface do usuário** > **Menu de contexto**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET NOD32 Antivirus no menu de contexto.

As seguintes opções estão disponíveis no menu suspenso **Tipo de menu**:

- **Completo (rastrear primeiro)** - Ativa todas as opções do menu de contexto; o menu principal exibirá a opção **Rastrear com ESET NOD32 Antivirus**.
- **Completo (limpar primeiro)** - Ativa todas as opções do menu de contexto; o menu principal exibirá a opção **Limpar com ESET NOD32 Antivirus**.
- **Apenas rastrear** - Somente a opção **Rastrear com ESET NOD32 Antivirus** será exibida no menu de contexto.
- **Apenas limpar** - Somente a opção **Limpar com ESET NOD32 Antivirus** será exibida no menu de contexto.

4.5.7 Modo de jogador

O modo de jogos é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Ao ativar esse recurso, todas as janelas pop-up são desativadas e a atividade da agenda será completamente interrompida. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

O modo de jogos pode ser ativado ou desativado na janela do programa principal clicando em **Configuração** > **Computador**; em seguida, em **Ativar** em **Modo de jogos**; ou pode ativar o Modo de jogos, na árvore Configuração avançada (F5), expandindo **Interface do usuário**, clicando em **Modo de jogos** e marcando a caixa de seleção ao lado de **Ativar modo de jogos**. Ativar automaticamente o modo de jogos é um risco de segurança em potencial, pois o ícone do status de proteção na barra de tarefas ficará laranja e exibirá um aviso. Esse aviso também pode ser visto na janela do programa principal, onde a opção Modo de jogos ativado será exibida em laranja.

Ao marcar a caixa de seleção **Ativar automaticamente o modo de jogos ao executar aplicativos em tela cheia**, o modo de jogos será iniciado depois que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Esse recurso é especialmente útil para iniciar o modo de jogos logo após iniciar um jogo, abrir um aplicativo em tela cheia ou iniciar uma apresentação.

Também é possível marcar a caixa de seleção **Desativar o modo de jogos automaticamente após X minutos** para definir o período de tempo após o qual o modo de jogos será desativado automaticamente (o valor padrão é 1 minuto).

5. Usuário avançado

5.1 Gerenciador de perfil

O gerenciador de perfil é usado em duas seções no ESET NOD32 Antivirus - **Rastrear o computador** e **Atualizar**.

Rastrear o computador

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Computador** > **Antivírus e antispyware** > **Rastrear o computador** > **Perfis...**. A janela **Perfis de configuração** inclui o menu suspenso **Perfil selecionado** que lista os perfis de rastreamento existentes e a opção para criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Digite o nome do novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil**. Depois, ajuste os demais parâmetros de maneira a atender as suas necessidades.

Atualizar

O editor de perfil na seção de configuração da Atualização permite que os usuários criem novos perfis de atualização. Crie e use os seus próprios perfis personalizados (isto é, outros que não sejam o padrão **Meu perfil**) somente se o seu computador usar diversos modos de conexão com os servidores de atualização.

Um exemplo é um laptop que normalmente se conecta ao servidor local de Imagem na rede local, mas faz os downloads das atualizações diretamente dos servidores de atualização da ESET quando está desconectado da rede local (em viagem de negócios, por exemplo). Nesse cenário, é adequado criar dois perfis: o primeiro conectando ao servidor local; o segundo aos servidores da ESET. Em seguida, navegue até **Ferramentas** > **Agenda** e edite os parâmetros da tarefa de atualização. Designe um perfil como primário e outro como secundário.

Perfil selecionado - O perfil de atualização atualmente usado. Para mudar, escolha um perfil no menu suspenso.

Adicionar... - Criar novos perfis de atualização.

A parte inferior da janela lista os perfis existentes.

5.2 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET NOD32 Antivirus incluem:

Ctrl+G	desativa a GUI no produto
Ctrl+I	abre a página do ESET SysInspector
Ctrl+L	abre a página Arquivos de log
Ctrl+S	abre a página Agenda
Ctrl+Q	abre a página Quarentena
Ctrl+U	abre a configuração de Nome de usuário e Senha
Ctrl+R	redefine a janela para seu tamanho e posição padrão na tela.

Para uma melhor navegação no produto de segurança ESET, os seguintes atalhos de teclado podem ser utilizados:

F1	abre as páginas da Ajuda
F5	abre a Configuração avançada
Up/Down	permite a navegação no produto por itens
*	expande o nó da árvore de Configuração avançada
-	recolhe os nós da árvore de Configuração avançada
TAB	move o cursor em uma janela
Esc	fecha a janela da caixa de diálogo ativa

5.3 Diagnóstico

O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, *ekrn*). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir os problemas do ESET NOD32 Antivirus. Estão disponíveis dois tipos de despejos:

- **Despejo de memória completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo pára inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.
- **Despejo de memória resumido** - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Esse tipo de arquivo de despejo pode ser útil quando o espaço é limitado. No entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- Selecione **Não gerar despejo de memória** (padrão) para desativar esse recurso.

Diretório de destino – Diretório no qual o despejo durante a falha será gerado. Clique em **Abrir pasta...** para abrir esse diretório em uma nova janela do *Windows explorer*.

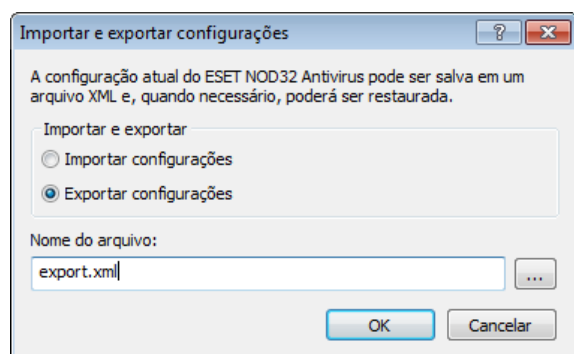
5.4 Importar e exportar configurações

Você pode importar ou exportar seu arquivo de configuração .xml personalizado do ESET NOD32 Antivirus do menu **Configuração**.

A importação e a exportação dos arquivos de configuração serão úteis caso precise fazer backup da configuração atual do ESET NOD32 Antivirus para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET NOD32 Antivirus em diversos sistemas. Os usuários podem importar facilmente um arquivo *.xml* para transferir essas configurações.

A importação de uma configuração é muito fácil. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações...** e selecione a opção **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão **...** para procurar o arquivo de configuração que deseja importar.

As etapas para exportar uma configuração são muito semelhantes. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações...**. Selecione a opção **Exportar configurações** e insira o nome de arquivo do arquivo de configuração (ou seja, *export.xml*). Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

Observação: Você pode encontrar um erro ao exportar configurações se não tiver direitos suficientes para gravar o arquivo exportado no diretório especificado.

5.5 Detecção em estado ocioso

As configurações da detecção em estado ocioso podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Detecção em estado ocioso**. Essas configurações especificam um acionador para Rastreamento em estado ocioso, quando:

- a proteção de tela estiver em execução,
- o computador estiver bloqueado,
- um usuário efetuar logoff.

Use as caixas de seleção acima para ativar ou desativar os acionadores de detecção de estado ocioso.

5.6 ESET SysInspector

5.6.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada nas soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões têm funções idênticas e os mesmos controles de programa. A única diferença é a forma como os resultados são gerenciados. As versões autônoma e integrada permitem exportar instantâneos do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os instantâneos do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator). Para mais informações, consulte a seção ESET SysInspector como parte do ESET NOD32 Antivirus.

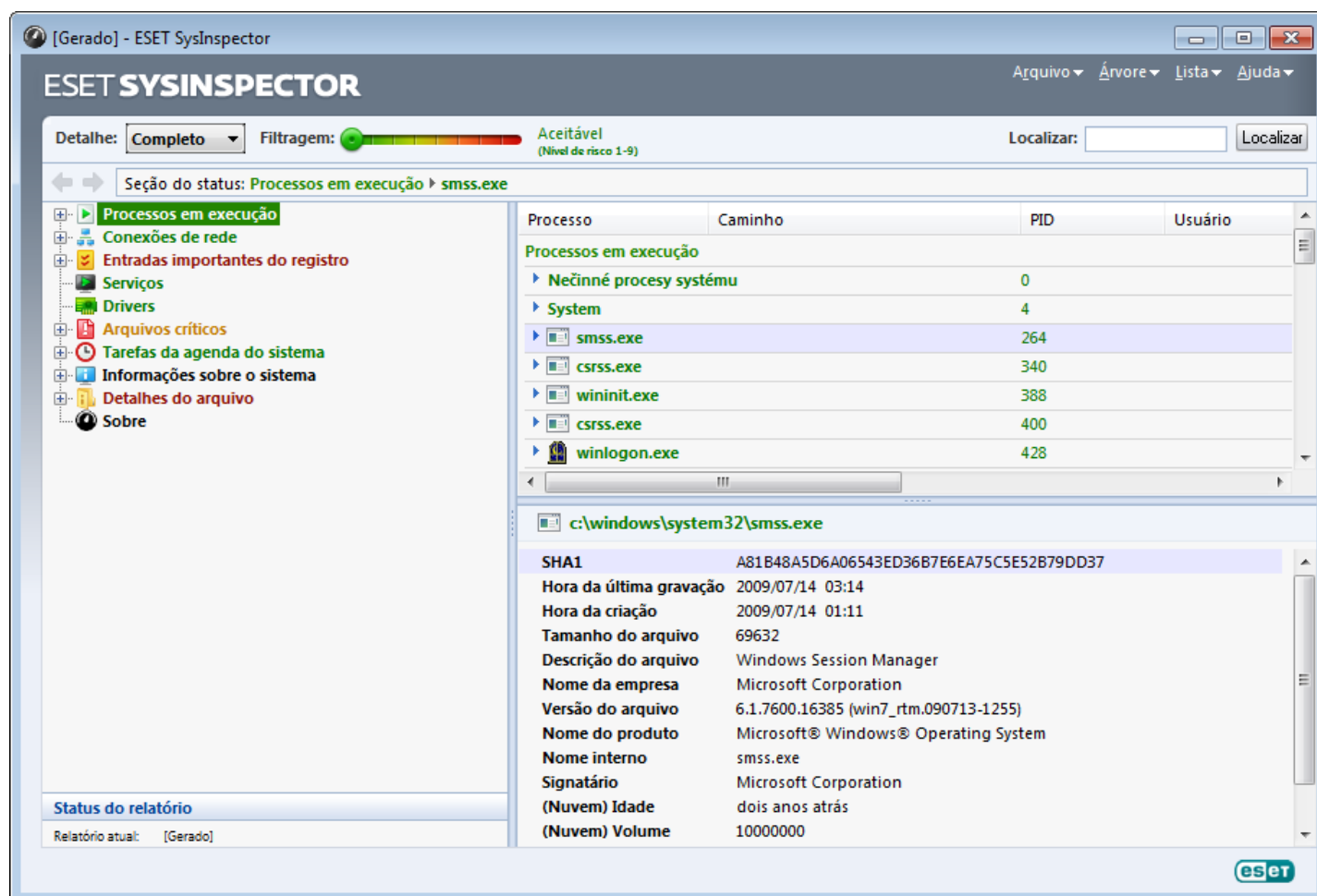
Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

5.6.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo executável *SysInspector.exe* obtido por download no site da ESET. Se já tiver uma das soluções ESET Security instalada, é possível executar o ESET SysInspector diretamente a partir do menu Iniciar (clique em **Programas** > **ESET** > **ESET NOD32 Antivirus**).

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos.

5.6.2 Interface do usuário e uso do aplicativo

Para maior clareza, a janela do programa principal é dividida em quatro seções principais - Controles do programa localizados na parte superior da janela do programa principal, a janela Navegação à esquerda, a janela Descrição à direita e a janela Detalhes, na parte inferior da janela do programa principal. A seção Status do log lista os parâmetros básicos de um log (filtro usado, tipo de filtro, se o log é o resultado de uma comparação, etc.).

5.6.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um log armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um log **Adequado para envio**. Neste formulário, o log omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente arrastando e soltando-os na janela do programa principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela do programa principal para facilitar o trabalho com as informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe detalhes menos usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para resolver problemas muito específicos.

Filtragem de itens

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver configurado todo para a esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante todo para a direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens identificados como de risco 6 a 9 podem colocar a segurança em risco. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrou esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Pesquisar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, certifique-se de que os arquivos são realmente perigosos ou desnecessários.

5.6.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer os itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do log. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo, o nível de risco do arquivo, etc.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados constantemente e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas freqüentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de Tarefas do Windows em uma hora/intervalo específico.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas, os direitos do usuário e os registros de eventos do sistema.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista dos módulos do programa.

5.6.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	Abre o log existente
Ctrl+S	Salva os logs criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	Aceitável, nível de risco 1-9, os itens são exibidos
2	Aceitável, nível de risco 2-9, os itens são exibidos
3	Aceitável, nível de risco 3-9, os itens são exibidos
4, U	Desconhecido, nível de risco 4-9, os itens são exibidos
5	Desconhecido, nível de risco 5-9, os itens são exibidos
6	Desconhecido, nível de risco 6-9, os itens são exibidos

7, B	Perigoso, nível de risco 7-9, os itens são exibidos
8	Perigoso, nível de risco 8-9, os itens são exibidos
9	Perigoso, nível de risco 9, os itens são exibidos
-	Diminui o nível de risco
+	Aumenta o nível de risco
Ctrl+9	Modo de filtragem, nível igual ou superior
Ctrl+0	Modo de filtragem, somente nível igual

Exibir

Ctrl+5	Exibição por fornecedor, todos os fornecedores
Ctrl+6	Exibição por fornecedor, somente Microsoft
Ctrl+7	Exibição por fornecedor, todos os outros fornecedores
Ctrl+3	Exibe detalhes completos
Ctrl+2	Exibe detalhes da mídia
Ctrl+1	Exibição básica
Backspace	Move um passo para trás
Espaço	Move um passo para a frente
Ctrl+W	Expande a árvore
Ctrl+Q	Recolhe a árvore

Outros controles

Ctrl+T	Vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	Exibe informações básicas sobre um item
Ctrl+A	Exibe informações completas sobre um item
Ctrl+C	Copia a árvore do item atual
Ctrl+X	Copia itens
Ctrl+B	Localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	Abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	Abre a entrada correspondente no editor do registro
Ctrl+Z	Copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	Alterna para o campo de pesquisa
Ctrl+D	Fecha os resultados da pesquisa
Ctrl+E	Executa script de serviços

Comparação

Ctrl+Alt+O	Abre o log original/comparativo
Ctrl+Alt+R	Cancela a comparação
Ctrl+Alt+1	Exibe todos os itens
Ctrl+Alt+2	Exibe apenas os itens adicionados; o log mostrará os itens presentes no log atual
Ctrl+Alt+3	Exibe apenas os itens removidos; o log mostrará os itens presentes no log anterior
Ctrl+Alt+4	Exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	Exibe apenas as diferenças entre os logs
Ctrl+Alt+C	Exibe a comparação
Ctrl+Alt+N	Exibe o log atual
Ctrl+Alt+P	Exibe o log anterior

Diversos

F1	Exibe a Ajuda
Alt+F4	Fecha o programa
Alt+Shift+F4	Fecha o programa sem perguntar
Ctrl+I	Estatísticas de logs

5.6.2.3 Comparar

O recurso Comparar permite que o usuário compare dois logs existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os logs. Ele é adequado se você desejar manter controle das alterações no sistema, uma ferramenta útil para detectar código malicioso.

Após ser iniciado, o aplicativo criará um novo log, que será exibido em uma nova janela. Clique em **Arquivo** > **Salvar relatório** para salvar um log em um arquivo. Os arquivos de log podem ser abertos e visualizados posteriormente. Para abrir um log existente, clique em **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um log de cada vez.

O benefício de comparar dois logs é que você pode visualizar um log ativo atual e um log salvo em um arquivo. Para comparar logs, clique em **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O log selecionado será comparado com o log ativo na janela principal do programa. O log comparativo exibirá somente as diferenças entre esses dois logs.

OBSERVAÇÃO: Caso compare dois arquivos de log, clique em **Arquivo** > **Salvar relatório** para salvá-lo como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir esse arquivo posteriormente, os logs contidos serão comparados automaticamente.

Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os logs comparados.

Os itens marcados por um - apenas podem ser encontrados no log ativo e não estavam presentes no log comparativo aberto. Os itens marcados por um + estavam presentes apenas no log aberto e estavam ausentes no log ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- + novo valor, não presente no log anterior
- a seção de estrutura em árvore contém novos valores
- - valor removido, presente apenas no log anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no log anterior
- o nível de risco aumentou / era menor no log anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos logs que estão sendo comparados.

Qualquer log comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois logs, clique em **Arquivo** > **Comparar relatórios**. O programa criará um log comparativo mostrando as diferenças entre os logs.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

5.6.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar um log diretamente a partir da linha de comando sem executar a GUI
/privacy	gerar um log excluindo informações confidenciais
/zip	armazenar o log resultante diretamente no disco em um arquivo compactado
/silent	ocultar a exibição da barra de progresso da geração de logs
/help, /?	exibir informações sobre os parâmetros da linha de comando

Exemplos

Para carregar um log específico diretamente no navegador, use: *SysInspector.exe "c:\clientlog.xml"*
Para gerar um log em um local atual, use: *SysInspector.exe /gen*
Para gerar um log em uma pasta específica, use: *SysInspector.exe /gen="c:\folder\"*
Para gerar um log em um arquivo/local específico, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para gerar um log que exclua informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dois logs, use: *SysInspector.exe "current.xml" "original.xml"*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

5.6.4 Script de serviços

O script de serviços é uma ferramenta que fornece ajuda aos clientes que utilizam o ESET SysInspector removendo facilmente os objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o log modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As modificações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador está infectado por um vírus que não é detectado pelo seu programa antivírus, siga estas instruções passo a passo:

1. Execute o ESET SysInspector para gerar um novo instantâneo do sistema.
2. Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Shift e selecione o último item para marcar todos os itens.
3. Clique com o botão direito do mouse nos objetos selecionados e selecione **Exportar as seções selecionadas para script de serviços**.
4. Os objetos selecionados serão exportados para um novo log.
5. Esta é a etapa mais crucial de todo o procedimento: abra o novo log e altere o atributo - para + em todos os objetos que desejar remover. Verifique se não marcou arquivos/objetos do sistema operacional importantes.
6. Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o script.
7. Clique em **OK** para executar o script.

5.6.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector . No menu de contexto, selecione **Exportar todas as seções para script de serviços** ou **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois logs estiverem sendo comparados.

5.6.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, pode encontrar informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do log (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e um título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Ao executar o script, os drivers selecionados serão parados. Observe que alguns drivers não permitirão serem parados.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos que são críticos para o funcionamento correto do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos ou redefinidos aos valores padrão originais.

5.6.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma janela de diálogo confirmará que o script foi executado com êxito.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

5.6.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um arquivo de log?

O ESET SysInspector pode criar um arquivo de log da configuração do computador. Para salvar um arquivo de log, clique em **Arquivo** > **Salvar relatório** na janela do programa principal. Os arquivos de log são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*, com uma convenção de nomenclatura de arquivos de "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Você pode alterar o local e o nome do

arquivo de log para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o arquivo de log do ESET SysInspector?

Para visualizar um arquivo de log criado pelo ESET SysInspector, execute o programa e clique em **Arquivo** > **Abrir relatório** na janela do programa principal. Você também pode arrastar e soltar arquivos de log no aplicativo ESET SysInspector. Se você precisar visualizar os arquivos de log do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os arquivos de log para visualização. Por motivo de segurança, o Windows Vista/7 pode não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do arquivo de log? E um SDK?

Atualmente, não há uma especificação para o arquivo de log nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 – Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro delas.

Um nível de risco "6 - Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles poderão querer examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporte como um rootkit, o usuário poderá ser exposto à perda ou ao roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validado usando essa informação. Se a assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Caso o arquivo CAT relevante seja encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Arquivos de Programas\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

5.6.6 ESET SysInspector como parte do ESET NOD32 Antivirus

Para abrir a seção do ESET SysInspector no ESET NOD32 Antivirus, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com instantâneos: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar ou excluir instantâneos, utilize os botões correspondentes localizados abaixo da lista de instantâneos na janela do ESET SysInspector . Essas opções também estão disponíveis no menu de contexto. Para exibir o instantâneo do sistema selecionado, selecione **Mostrar** no menu de contexto. Para exportar o instantâneo selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**

Abaixo, veja uma descrição detalhada das opções disponíveis:

- **Comparar** - Permite comparar dois logs existentes. Ela é adequada se você desejar controlar alterações entre o log atual e um log anterior. Para que essa opção entre em vigor, é necessário selecionar dois instantâneos a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para saber mais sobre o progresso de criação de instantâneos (do instantâneo gerado no momento), consulte a coluna **Status**. Todos os instantâneos concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** – Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

5.7 ESET SysRescue

O ESET SysRescue é um utilitário que permite a criação de um disco de inicialização contendo uma das soluções ESET Security, podendo ser o ESET NOD32 Antivirus, o ESET Smart Security ou até mesmo algum dos produtos orientados ao servidor. A principal vantagem do ESET SysRescue é o fato de a solução ESET Security ser executada de maneira independente do sistema operacional host, possuindo ao mesmo tempo um acesso direto ao disco e a todo o sistema de arquivos. Isso permite remover infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

5.7.1 Requisitos mínimos

O ESET SysRescue funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista.

O Windows PE faz parte do pacote gratuito Windows Automated Installation Kit (Windows AIK). O Windows AIK deve ser instalado antes da criação do ESET SysRescue (http://go.eset.eu/AIK). Devido ao suporte da versão de 32 bits do Windows PE, é necessário usar o pacote de instalação de 32 bits da solução ESET Security ao criar o ESET SysRescue em sistemas de 64 bits. O ESET SysRescue é compatível com o Windows AIK 1.1 e versões posteriores.

OBSERVAÇÃO: Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download.

O ESET SysRescue está disponível nas soluções ESET Security 4.0 e versões posteriores.

Sistemas operacionais compatíveis

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 com KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 com KB926044
- Windows XP Service Pack 3

5.7.2 Como criar o CD de restauração

Para iniciar o assistente do ESET SysRescue, clique em **Iniciar** > **Programas** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK e de um dispositivo adequado para a criação da mídia de inicialização. Se o Windows AIK não estiver instalado no computador (ou estiver corrompido ou instalado incorretamente), o assistente dará a opção de instalá-lo ou de inserir o caminho para a pasta do Windows AIK (http://go.eset.eu/AIK).

OBSERVAÇÃO: Como o Windows AIK é maior que 1 GB, uma conexão com a Internet de alta velocidade é necessária para um download.

Na próxima etapa, selecione a mídia de destino em que o ESET SysRescue estará localizado.

5.7.3 Seleção de alvos

Além de CD/DVD/USB, você pode escolher salvar o ESET SysRescue em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VMWare ou VirtualBox).

Se você selecionar USB como a mídia-alvo, a reinicialização pode não funcionar em determinados computadores. Algumas versões de BIOS podem relatar problemas com o BIOS - comunicação com o gerenciador de inicialização (por exemplo, no Windows Vista), e a inicialização é encerrada com a seguinte mensagem de erro:

```
arquivo: \boot\bcd
status: 0xc000000e
informações: an error occurred while attemping to read the boot configuration data (ocorreu um erro ao tenta
```

Se você encontrar essa mensagem, recomendamos que selecione o CD, em vez da mídia USB.

5.7.4 Configurações

Antes de iniciar a criação do ESET SysRescue, o assistente de instalação exibe os parâmetros de compilação. Para modificá-los, clique no botão **Alterar...**. As opções disponíveis incluem:

- Pastas
- Antivírus ESET
- Avançado
- Protoc. Internet
- Dispositivo USB inicializável (quando o dispositivo USB de destino é selecionado)
- Gravação (quando a unidade de CD/DVD de destino é selecionada)

A opção **Criar** estará inativa se nenhum pacote de instalação MSI for especificado ou se nenhuma solução ESET Security estiver instalada no computador. Para selecionar um pacote de instalação, clique em **Alterar** e clique na guia **Antivírus ESET**. Além disso, se você não preencher o nome do usuário e a senha (**Alterar** > **Antivírus ESET**), a opção **Criar** estará acinzentada.

5.7.4.1 Pastas

A **Pasta temporária** é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

Pasta ISO é uma pasta, em que o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas das pastas estiverem localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode terminar prematuramente devido a espaço livre em disco insuficiente.

Aplicativos externos - Permite especificar os programas adicionais que serão executados ou instalados após a inicialização a partir de uma mídia do ESET SysRescue.

Incluir aplicativos externos - Permite adicionar programas externos à compilação do ESET SysRescue.

Pasta selecionada - Pasta na qual os programas a serem adicionados ao disco do ESET SysRescue estão localizados.

5.7.4.2 Antivírus ESET

Para criar o CD do ESET SysRescue, é possível selecionar entre duas fontes de arquivos da ESET para serem utilizadas pelo compilador:

Pasta do ESS/EAV - Arquivos já contidos na pasta na qual a solução ESET Security está instalada no computador.

Arquivo MSI - São usados os arquivos contidos no instalador do MSI.

Em seguida, é possível atualizar a localização dos arquivos (.nup). Normalmente, a opção padrão **Pasta do ESS/EAV/ Arquivo MSI** deve ser selecionada. Em alguns casos, uma **Pasta de atualização** personalizada pode ser definida, por exemplo, para usar uma versão mais antiga ou mais recente de um banco de dados de assinatura de vírus.

É possível utilizar uma das seguintes fontes de nome de usuário e senha:

ESS/EAV instalado - O nome de usuário e a senha são copiados da solução ESET Security instalada no momento.

Do usuário - O nome de usuário e a senha digitados nos campos correspondentes serão utilizados.

OBSERVAÇÃO: A solução ESET Security no CD do ESET SysRescue é atualizada a partir da Internet ou da solução ESET Security instalada no computador em que o CD do ESET SysRescue for executado.

5.7.4.3 Configurações avançadas

A guia **Avançado** permite otimizar o CD do ESET SysRescue de acordo com o tamanho da memória do computador. Selecione **576 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 576 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Na seção **Drivers externos**, é possível inserir drivers para o seu hardware específico (geralmente o adaptador de rede). Embora o WinPE seja baseado no Windows Vista SP1, que suporta uma larga escala de hardware, algumas vezes o hardware não é reconhecido. Isso requer que o driver seja adicionado manualmente. Há duas maneiras de inserir o driver em uma compilação do ESET SysRescue: manualmente (clique em **Adicionar**) e automaticamente (clique em **Pesquisa automática**). No caso de inserção manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). No caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador específico. Recomendamos que use a inserção automática apenas se o ESET SysRescue for usado em um computador com o mesmo adaptador de rede usado no computador em que o CD ESET SysRescue foi criado. Durante a criação, o driver do ESET SysRescue é inserido na compilação para que você não precise procurá-lo depois.

5.7.4.4 Protoc. Internet

Essa seção permite configurar informações básicas de rede e definir as conexões predefinidas após a execução do ESET SysRescue.

Selecione **Endereço IP privado autom.** para obter o endereço IP automaticamente a partir do servidor DHCP (Dynamic Host Configuration Protocol, protocolo de configuração dinâmica de endereços de rede).

Se preferir, a conexão de rede pode usar um endereço IP especificado manualmente (também conhecido como endereço IP estático). Selecione **Personalizar** para definir as configurações adequadas para o endereço IP. Ao definir essa opção, é preciso especificar um **Endereço IP** e, para a LAN e as conexões de Internet de alta velocidade, uma **Máscara de sub-rede**. Em **Servidor DNS preferencial** e **Servidor DNS alternativo**, digite os endereços principal e secundário do servidor DNS.

5.7.4.5 Dispositivo USB inicializável

Se você selecionou um dispositivo USB como mídia-alvo, é possível selecionar um dos dispositivos USB disponíveis na guia **Dispositivo USB inicializável** (caso haja mais dispositivos USB).

Selecione o **Dispositivo** de destino apropriado onde o ESET SysRescue será instalado.

Aviso: O dispositivo USB selecionado será formatado durante a criação do ESET SysRescue. Todos os dados no dispositivo serão excluídos.

Se você selecionar **Formatação rápida**, a formatação removerá todos os arquivos da partição, mas não rastreará o disco em busca de setores corrompidos. Use essa opção se o dispositivo USB tiver sido formatado anteriormente e você tiver certeza de que ele não está danificado.

5.7.4.6 Gravar

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia **Gravar**.

Excluir arquivo ISO - Selecione para excluir o arquivo ISO temporário após o CD do ESET SysRescue ser criado.

Exclusão ativada - Permite selecionar o apagamento rápido e concluí-lo.

Dispositivo de gravação - Selecione a unidade a ser utilizada para gravação.

Aviso: Essa é a opção padrão. Se um CD/DVD regravável for usado, todos os dados contidos no CD/DVD serão apagados.

A seção Mídia contém informações sobre a mídia no seu dispositivo de CD/DVD.

Velocidade de gravação - Selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser considerados ao selecionar a velocidade da gravação.

5.7.5 Trabalhar com o ESET SysRescue

Para o CD/DVD/USB de restauração funcionar de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Como alternativa, você pode usar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas: F9 a F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização da mídia de inicialização, a solução ESET Security será iniciada. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos do programa presentes na versão padrão da solução ESET Security não são necessários; a lista é limitada ao **Rastrear o computador**, à opção **Atualizar**, e algumas seções da **Configuração**. A capacidade de atualizar o banco de dados de assinaturas de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastrear o computador.

5.7.5.1 Utilização do ESET SysRescue

Suponha que os computadores na rede tenham sido infectados por um vírus que modifica os arquivos executáveis (. exe). A solução ESET Security consegue limpar todos os arquivos infectados, exceto o *explorer.exe*, que não pode ser limpo, mesmo no modo de segurança. Isso ocorre porque o *explorer.exe*, como um dos processos essenciais do Windows, também é iniciado no modo de segurança. A solução ESET Security não poderia realizar ações com o arquivo e ele permaneceria infectado.

Nesse tipo de cenário, seria possível usar o ESET SysRescue para solucionar o problema. O ESET SysRescue não requer componentes do sistema operacional host, portanto ele pode processar (limpar, excluir) qualquer arquivo no disco.

5.8 Linha de comando

O módulo antivírus do ESET NOD32 Antivirus pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat"). Uso para o rastreamento por linha de comando da ESET:

```
ecls [OPTIONS..] FILES..
```

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções

/base-dir=PASTA	carregar módulos da PASTA
/quar-dir=PASTA	PASTA de quarentena
/exclude=MÁSCARA	excluir arquivos que correspondem à MÁSCARA do rastreamento
/subdir	rastrear subpastas (padrão)
/no-subdir	não rastrear subpastas
/max-subdir-level=NÍVEL	subnível máximo de pastas dentro de pastas para rastrear
/symlink	seguir links simbólicos (padrão)
/no-symlink	ignorar links simbólicos
/ads	rastrear ADS (padrão)
/no-ads	não rastrear ADS
/log-file=ARQUIVO	registrar o relatório em ARQUIVO
/log-rewrite	substituir arquivo de saída (padrão - acrescentar)

/log-console	registrar saída para console (padrão)
/no-log-console	não registrar saída para console
/log-all	também registrar arquivos limpos
/no-log-all	não registrar arquivos limpos (padrão)
/aind	mostrar indicador de atividade
/auto	rastrear e limpar automaticamente todos os discos locais

Opções do scanner

/files	rastrear arquivos (padrão)
/no-files	não rastrear arquivos
/memory	rastrear memória
/boots	rastrear setores de inicialização
/no-boots	não rastrear setores de inicialização (padrão)
/arch	rastrear arquivos compactados (padrão)
/no-arch	não rastrear arquivos compactados
/max-obj-size=TAMANHO	rastrear apenas arquivos com menos de TAMANHO megabytes (padrão 0 = sem limite)
/max-arch-level=NÍVEL	subnível máximo de arquivos dentro de arquivos (arquivos aninhados) para rastrear
/scan-timeout=LIMITE	rastrear arquivos pelo LIMITE máximo de segundos
/max-arch-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado se eles tiverem menos de TAMANHO (padrão 0 = sem limite)
/max-sfx-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado de auto-extração se eles tiverem menos de TAMANHO megabytes (padrão 0 = sem limite)
/mail	rastrear arquivos de email (padrão)
/no-mail	não rastrear arquivos de email
/mailbox	rastrear caixas de correio (padrão)
/no-mailbox	não rastrear caixas de correio
/sfx	rastrear arquivos compactados de auto-extração (padrão)
/no-sfx	não rastrear arquivos compactados de auto-extração
/rtp	rastrear empacotadores em tempo real (padrão)
/no-rtp	não rastrear empacotadores em tempo real
/adware	rastrear se há Adware/Spyware/Riskware (padrão)
/no-adware	não rastrear se há Adware/Spyware/Riskware
/unsafe	rastrear por aplicativos potencialmente inseguros
/no-unsafe	não rastrear por aplicativos potencialmente inseguros (padrão)
/unwanted	rastrear por aplicativos potencialmente indesejados
/no-unwanted	não rastrear por aplicativos potencialmente indesejados (padrão)
/pattern	usar assinaturas (padrão)
/no-pattern	não usar assinaturas
/heur	ativar heurística (padrão)
/no-heur	desativar heurística
/adv-heur	ativar heurística avançada (padrão)
/no-adv-heur	desativar heurística avançada
/ext=EXTENSÕES	verificar somente EXTENSÕES delimitadas por dois pontos
/ext-exclude=EXTENSÕES	excluir do rastreamento EXTENSÕES delimitadas por dois pontos
/clean-mode=MODO	utilizar MODO de limpeza para objetos infectados. Opções disponíveis: none (nenhum), standard (padrão), strict (rígida), rigorous (rigorosa), delete (excluir)
/quarantine	copiar arquivos infectados para Quarentena (completa a ação realizada enquanto ocorre a limpeza)
/no-quarantine	não copiar arquivos infectados para Quarentena

Opções gerais

/help	mostrar ajuda e sair
/version	mostrar informações de versão e sair
/preserve-time	manter último registro de acesso

Códigos de saída

0	nenhuma ameaça encontrada
1	ameaça encontrada e removida
10	alguns arquivos não puderam ser rastreados (podem conter ameaças)
50	ameaça encontrada
100	erro

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

6. Glossário

6.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

6.1.1 Vírus

Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro. Quanto ao termo "vírus", ele é frequentemente usado de maneira incorreta para significar qualquer tipo de ameaça. Essa utilização está gradualmente sendo superada e substituída por um termo mais preciso "malware" (software malicioso).

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o código malicioso é chamado e executado antes da execução do aplicativo original. Um vírus pode infectar qualquer arquivo que tenha permissão de gravação dada pelo usuário.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

Se o computador estiver infectado com um vírus e a limpeza não for possível, envie-o para o laboratório da ESET para análise. Em certos casos os arquivos infectados podem ser modificados a ponto de uma limpeza não ser possível e os arquivos precisarem ser substituídos por uma cópia limpa.

6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se propagar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms propagam-se para os endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de horas ou mesmo minutos após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

6.1.3 Cavalos de Troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de ameaças que tentam se apresentar como programas úteis, enganando assim os usuários para executá-los.

Dado que Cavalos de Troia são uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** - Programas maliciosos com a capacidade de fazer o download de outras ameaças da Internet.
- **Dropper** - Programas maliciosos com a capacidade para instalar outros tipos de malware em computadores comprometidos.
- **Backdoor** - Programas maliciosos que se comunicam com atacantes remotos, permitindo que eles acessem o computador e assumam o seu controle.
- **Keylogger** - (keystroke logger) - Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- **Dialer** - Programas maliciosos projetados para se conectar aos números premium-rate em vez do provedor de serviços de Internet do usuário. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.

Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele contém códigos maliciosos.

6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1. Quando eles tentam acessar um sistema: Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2. Quando eles estão ocultos para os testes usuais: os usuários do ESET NOD32 Antivirus têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

6.1.5 Adware

Adware é abreviação de “advertising-supported software” (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage do mesmo. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

6.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

6.1.7 Empacotadores

O empacotador é um executável de extração automática do tempo de execução que realiza vários tipos de malware em um único pacote.

Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Os empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando mais difícil a detecção e remoção do malware.

6.1.8 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET NOD32 Antivirus fornece a opção de detectar tais ameaças.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

6.1.9 Aplicativos potencialmente indesejados

Os **Aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento antes da instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- Novas janelas que você não via anteriormente (pop-ups, ads).
- Ativação e execução de processos ocultos.
- Uso aumentado de recursos do sistema.
- Alterações nos resultados de pesquisa.
- O aplicativo comunica-se com servidores remotos.

6.2 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. Flexível, rápido e direto, o email teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso - malware (códigos maliciosos). A inconveniência e o perigo para você são aumentados pelo fato de que os custos de envio são mínimos e os autores de spam têm muitas ferramentas para obter novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou à sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" - por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

6.2.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são o custo mínimo e um alto nível de objetividade. Além disso, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse tipo de publicidade é legítimo, desde que você tenha interesse em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o limite razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Geralmente, os autores dos emails não solicitados tentam mascarar o spam como mensagens legítimas.

6.2.2 Hoaxes

Um hoax é uma informação incorreta que é propagada pela Internet. Normalmente, os hoaxes são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

6.2.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por ex. instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

6.2.4 Reconhecimento de fraudes em spam

Geralmente, há alguns indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- O endereço do remetente não pertence a alguém da sua lista de contatos.
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma.
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais (números de contas bancárias, nomes de usuário e senhas, etc.)
- Está escrito em um idioma estrangeiro.
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo, "vaigra" em vez de "viagra", etc.